

EXHIBITS 2A-2H

EXHIBIT 2A

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

TEXTILE COMPUTER SYSTEMS, INC.,

Plaintiff,

v.

BROADWAY NATIONAL BANK D/B/A
BROADWAY BANK,

Defendant.

CIVIL ACTION NO. 6:21-cv-1050

ORIGINAL COMPLAINT FOR
PATENT INFRINGEMENT

JURY TRIAL DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Textile Computer Systems, Inc. (“Textile” or “Plaintiff”) files this original complaint against Defendant Broadway National Bank d/b/a Broadway Bank (“Broadway”), alleging, based on its own knowledge as to itself and its own actions and based on information and belief as to all other matters, as follows:

PARTIES

1. Textile Computer Systems, Inc. is a corporation formed under the laws of the State of Texas, with a place of business at 618 Bluff Trail, San Antonio, Texas, 78216.
2. Broadway National Bank d/b/a Broadway Bank is a national bank with its principal place of business at 1177 N.E. Loop 410, San Antonio, Texas 78209.
3. Broadway and its affiliates lead and are part of an interrelated group of companies which together comprise one of the country’s largest banking and financial service entities, including under the Broadway brand.

4. Broadway and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

5. Broadway and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

6. Broadway and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

7. Thus, Broadway and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.



JURISDICTION AND VENUE

8. This is an action for infringement of United States patents arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. § 1331 and § 1338(a).

9. This Court has personal jurisdiction over Broadway pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Broadway has done and continues to do business in Texas; and (ii) Broadway has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations, inducing others to commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein.

10. Venue is proper in this district pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Broadway has committed and continues to commit acts of patent infringement in this district. For example, Broadway cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those cardholders make and/or use the accused instrumentalities in the district. Broadway induces others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. Broadway has regular and established places of business in this district, including at least at 401 Austin Highway, San Antonio, Texas 78209, and at numerous other locations in and around San Antonio and Austin:

[LOCATIONS](#) [ABOUT US](#) [CONTACT US](#) [SIGN IN](#) [Q](#) [J](#)

Before visiting your local financial center, please call ahead for lobby availability and hours of operation.

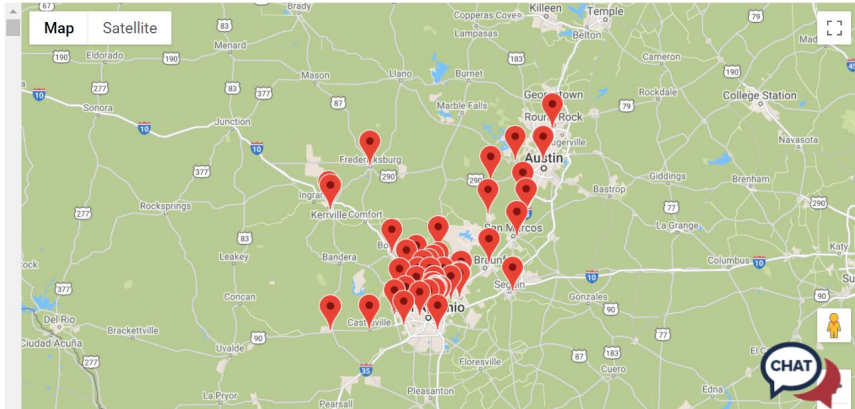
ATM & Bank Locations

1 Alamo Heights Financial Center

401 Austin Highway
San Antonio, TX 78209
(210) 283-6500

Drive Thru
Mon-Fri: 8 a.m. - 6 p.m.
Saturday: 9 a.m. - 1 p.m.

ATM



(Source: <https://broadway.bank/locations>)



(Source: screenshot from Google Maps Street View)

BACKGROUND

11. The patents-in-suit generally pertain to payment authorization technology used in payment networks used to process transactions from, for example, credit cards and debit cards. The technology disclosed by the patents was developed by Gopal Nandakumar, a Texas-based entrepreneur, software engineer, and prolific inventor with over 30 years of experience in the field of Information Management Systems.

12. In 1987, after receiving Master's Degrees from both the University of Madras, India and the Georgia Institute of Technology, Mr. Nandakumar formed Textile Computer Systems, Inc. ("Textile") for the purpose of consulting and developing software for the textile industry. In 2005, Textile began transitioning into credit card transaction systems. In 2011, Textile began to develop and market the MySingleLink suite of applications.

13. The Nandakumar patents are related to payment authorization technology. Mr. Nandakumar has been at the forefront of payment authorization, developing, disclosing, and patenting solutions for reducing fraud in credit and debit card transactions. Indeed, the

Nandakumar patents (or the applications leading to them) have been cited during patent prosecution over a hundred times, including by numerous leading companies in the payment authorization industry such as ADP, Bank of America, Google, Groupon, IBM, Mastercard, NEC, Paypal, Visa, and Wells Fargo.

THE TECHNOLOGY

14. The patents-in-suit, U.S. Patent Nos. 8,505,079, 8,533,802, 9,584,499, 10,148,659, and 10,560,454 (collectively, the “Asserted Patents”), teach systems, including payment processing systems, for securely and effectively approving and processing specific credit card and/or debit card transactions. Through the specific use of servers, messaging gateways, and/or interfaces, these systems act to reduce credit card and/or debit card fraud and misuse through their use and validation of key strings, authentication credentials, transaction specific information, and transaction specific credentials. The technology in the Asserted Patents improves the underlying functionality of existing card processing infrastructure by minimizing fraud and data theft in the face of attacks on payment systems that continue to grow in their number and sophistication.

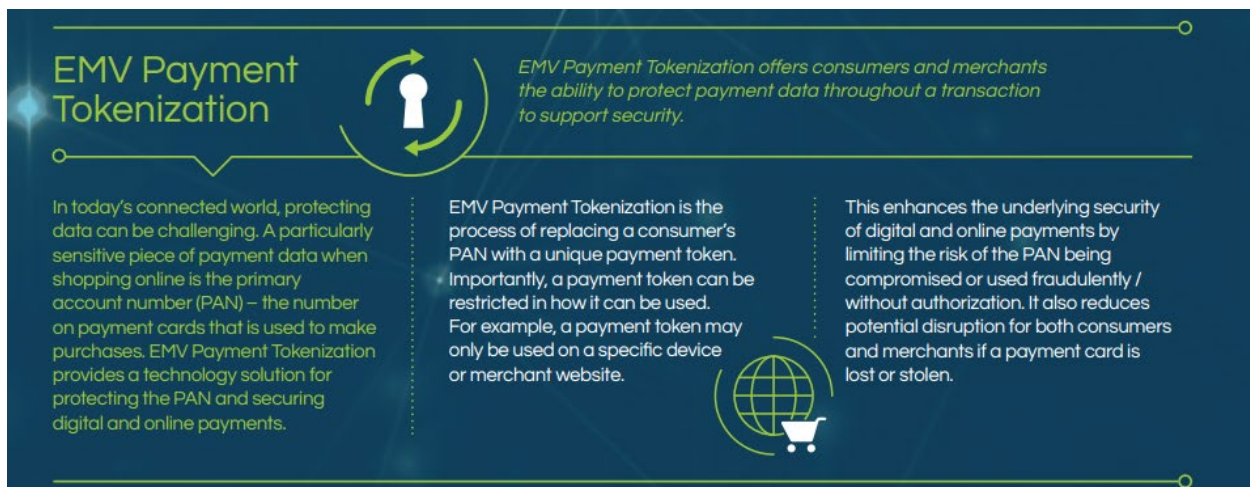
15. The patented improvements are critical for implementing secure payment systems, especially in light of the many high-profile merchant data breaches that have led to increased credit and debit card fraud. For example, in 2006, TJX Companies, who owns retailers like TJMaxx and Marshall’s, was hit with a cyber attack that resulted in the theft of credit cards leading to over \$100 million in fraud losses. In 2013, five people were indicted for attacking a number of retailers and financial institutions including NASDAQ, 7-Eleven, JCP, and others, stealing over 160 million cards. Also in 2013, the retailer Target suffered a data breach that resulted in 40 million debit and credit cards being compromised.

16. One implementation of the technology claimed in the Asserted Patents has been described by EMVCo as “a global Payment Tokenisation ecosystem that overlays and interoperates with existing payment ecosystems to support digital commerce and new methods of payment” and as “enhanc[ing] the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorized or fraudulent use of PANs.”

(Source: <https://www.emvco.com/emv-technologies/payment-tokenisation/>).

17. The technology claimed in the Asserted Patents is far from conventional technology. The payment industry gathered and consulted experts who worked together over a number of years to develop infringing payment tokenisation systems. In other words, the technology claimed in the Asserted Patents was not existing or conventional technology that the payment industry had sitting on the shelf.

18. Indeed, as recently as February of this year, EMVCo itself recognized that an implementation of the technology claimed in the Asserted Patents “provides a technology solution for protecting the PAN and securing digital and online payments”:



(Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

19. That same EMVCo document notes that “In today’s connected world, protecting data can be challenging. A particularly sensitive piece of payment data when shopping online is the primary account number (PAN) – the number on payment cards that is used to make purchases” and that EMVCo’s payment tokenization “enhances the underlying security of digital and online payments by limiting the risk of the PAN being compromised or used fraudulently / without authorization.” The document also states that the “Payment Tokenisation Specification provides an interoperable Technical Framework.” (Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

20. One of the asserted patents, the 079 Patent, was challenged in an Inter Partes Review proceeding before the Patent and Trademark Office (“PTO”). The PTO found that the challenger, Unified Patents Inc., was unable to show that one element, the “key string” as claimed in the 079 Patent claims and as construed by the PTO, was in the prior art at all, much less it being conventional or widespread. The PTO thus confirmed the patentability of all challenged claims of the 079 Patent.

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 8,505,079

21. On August 6, 2013, United States Patent No. 8,505,079 (“the 079 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

22. Textile is the owner of the 079 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 079 Patent against infringers, and to collect damages for all relevant times.

23. Broadway offers debit and/or credit cards, such as the Broadway Bank Visa Contactless Debit Card, that are used with an authentication system that authenticates the identity of a Broadway card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Broadway card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities, for example. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.



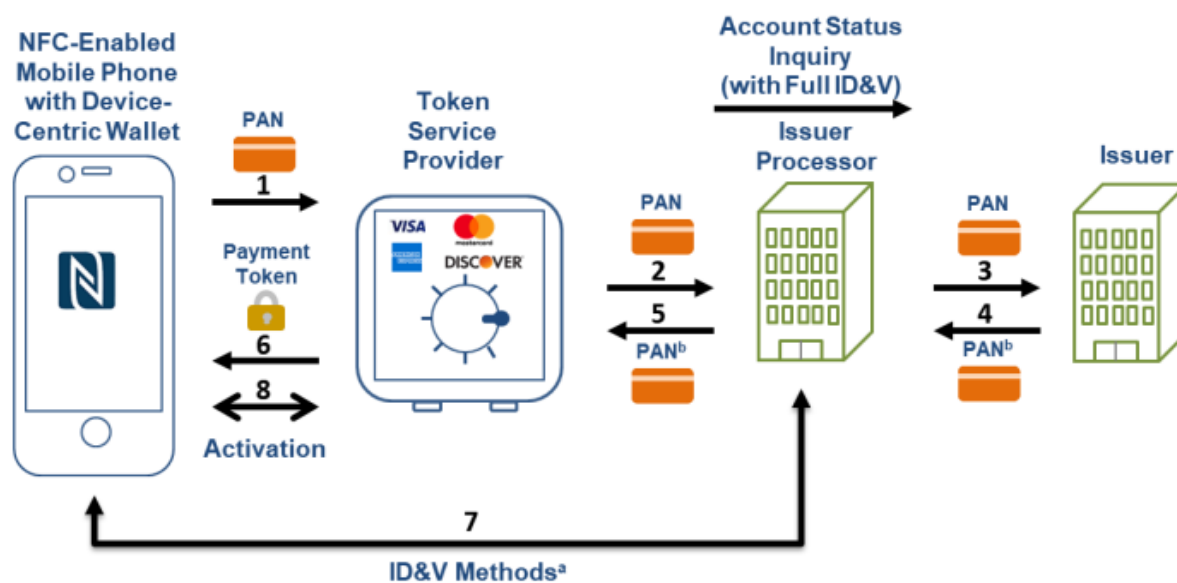
Pay with Your Hand-held Device

Your Broadway Bank Visa® Debit card is digital wallet ready. Digital wallets are a great way to virtually load a physical card into a mobile app and store it for fast, easy access at the point of sale. You can use this feature with Apple Pay®, Google Pay®, and Samsung Pay®.

(Source: <https://broadway.bank/personal/checking-savings/tools/debit-card>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^a ID&V methods includes text or email or call. OTP is an example.

^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

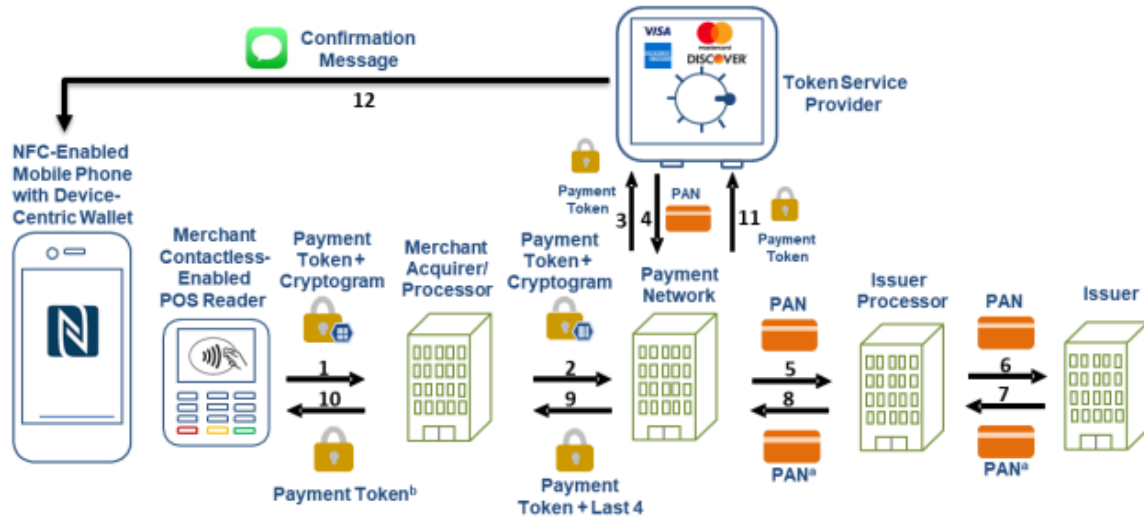
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

24. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a Broadway account holder requests Broadway to provision a specific Broadway debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Broadway card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's

smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

25. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Broadway card account holders for provisioning a specific Broadway debit and/or credit card for use on their mobile devices. The messaging gateway is also programmed to receive requests initiated by Broadway card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Broadway card account of the account holder. This messaging gateway is either hosted directly by Broadway or through an agent with whom Broadway has contracted to receive the messages.

26. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to determine a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the messaging

gateway and in secure communication therewith is an authorization server that processes the received request to identify the token value sent for the account selected to be charged that was passed from the authorized user to the merchant terminal via the NFC communication link. From the token value, the server can look up the debit and/or credit card account number. The authorization server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to provide the authentication services.

27. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive within the payment authorization request transaction specific information that was input into the request by the merchant. The interface is either hosted directly by Broadway or through an agent with whom Broadway has contracted to provide the authentication services.

28. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

29. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

30. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

31. Defendants thus infringe one or more of the claims of the 079 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 079 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 079 Patent.

32. Broadway has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(a), by making, using, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

33. Broadway has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 079 Patent by others and Broadway will continue to do so unless enjoined by this Court. Broadway's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors,

agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 079 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Broadway knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 079 Patent.

34. Broadway continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 079 Patent.

35. Broadway has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 079 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

36. Broadway has committed these acts of infringement without license or authorization.

37. By engaging in the conduct described herein, Broadway has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Broadway is thus liable to Textile for infringement of the 079 Patent, pursuant to 35 U.S.C. § 271.

38. As a direct and proximate result of Broadway's infringement of the 079 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Broadway's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

39. In addition, the infringing acts and practices of Broadway have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Broadway is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Broadway is finally and permanently enjoined from further infringement.

40. Broadway has had actual knowledge of the 079 Patent at least as of October 18, 2013, when Textile sent a letter to James D. Goudge, then Chief Executive Officer of Broadway Bank, that described certain implementations of the patented technology and specifically identified the 079 Patent.

41. Broadway has had actual knowledge of the 079 Patent at least as of October 25, 2013, when Textile sent a letter to Jeff Foote, then Executive Vice President of Broadway Bank,

that described certain implementations of the patented technology and specifically identified the 079 Patent.

42. Broadway has had actual knowledge of the 079 Patent at least as of November 10, 2014, when Textile sent two letters – one to James D. Goudge, then Chief Executive Officer of Broadway Bank, and one to Jeff Foote, then Executive Vice President of Broadway Bank, that described certain implementations of the patented technology and specifically identified the 079 Patent.

43. Broadway has had actual knowledge of the 079 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Broadway will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 079 Patent.

44. Broadway has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 079 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

45. Textile has been damaged as a result of the infringing conduct by Broadway alleged above. Thus, Broadway is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

46. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 079 Patent.

COUNT II

INFRINGEMENT OF U.S. PATENT NO. 8,533,802

47. On September 10, 2013, United States Patent No. 8,533,802 (“the 802 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

48. Textile is the owner of the 802 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 802 Patent against infringers, and to collect damages for all relevant times.

49. Broadway offers debit and/or credit cards, such as the Broadway Bank Visa Contactless Debit Card, that are used with an authentication system that authenticates the identity of a Broadway card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Broadway card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.



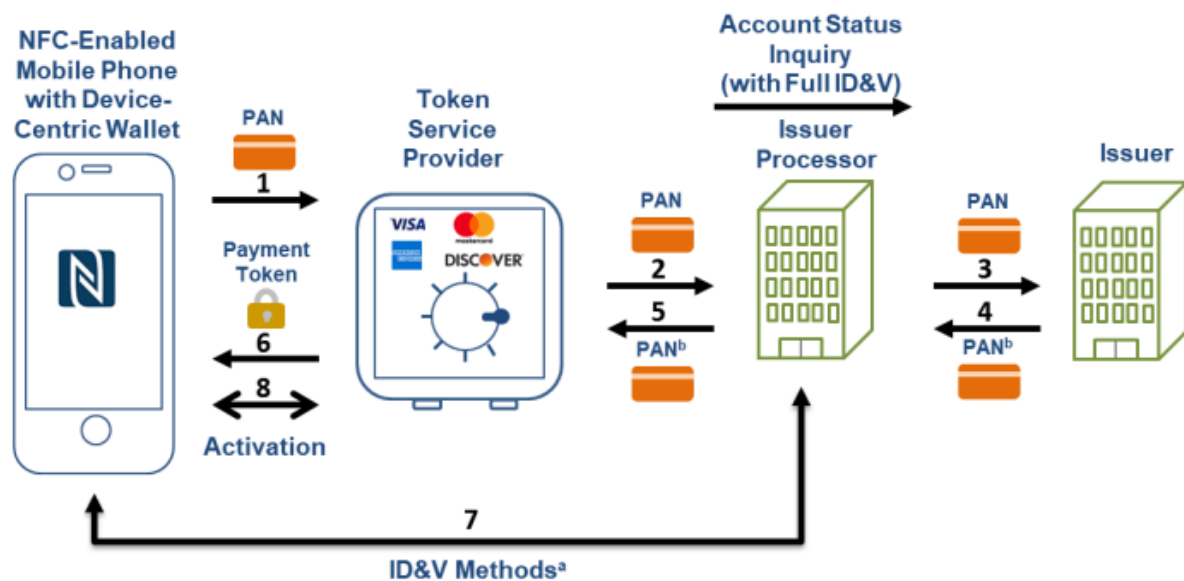
Pay with Your Hand-held Device

Your Broadway Bank Visa® Debit card is digital wallet ready. Digital wallets are a great way to virtually load a physical card into a mobile app and store it for fast, easy access at the point of sale. You can use this feature with Apple Pay®, Google Pay® and Samsung Pay®.

(Source: <https://broadway.bank/personal/checking-savings/tools/debit-card>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^a ID&V methods includes text or email or call. OTP is an example.

^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

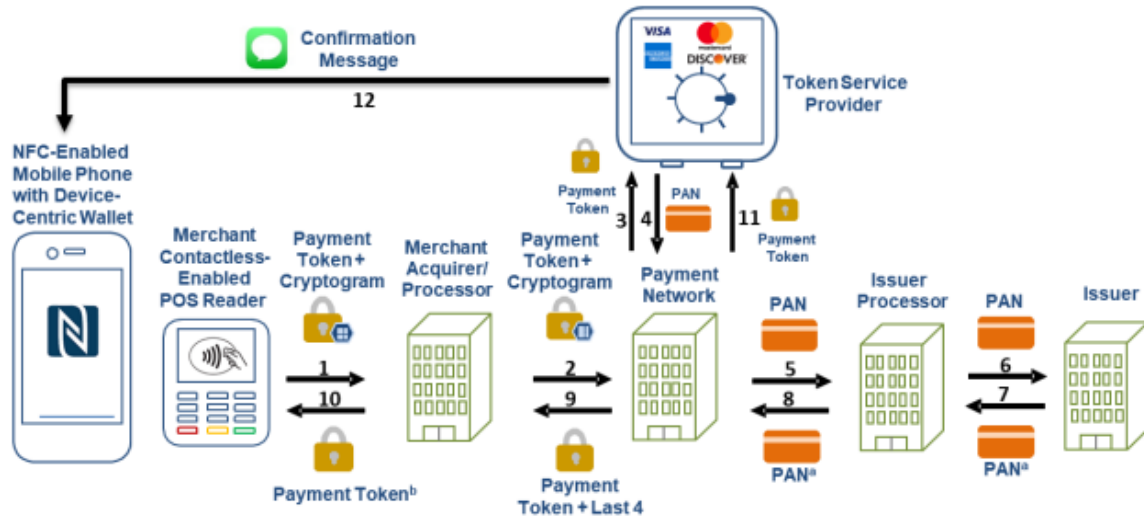
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

50. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a Broadway account holder requests Broadway to provision a specific Broadway debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Broadway card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's

smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

51. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Broadway card account holders for provisioning a specific Broadway debit and/or credit card for use on their mobile devices. This messaging gateway is either hosted directly by Broadway or through an agent with whom Broadway has contracted to receive the messages.

52. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate a key string adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the message gateway and in secure communication therewith is an authorization server that generates a token corresponding to the debit and/or credit card account number. The authorization server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to provide the authentication services.

53. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive transaction specific information that was input into the request by the merchant, *e.g.*, the merchant ID, invoice number, invoice amount, and date/timestamp. The interface is either hosted directly by Broadway or through an agent with whom Broadway has contracted to provide the authentication services.

54. The Accused Instrumentality includes a first set of instructions further operable to communicate the key string to the authorized user that the requester purports to be. For example, the messaging gateway sends the generated token to the authorized user's mobile device for use in merchant transactions.

55. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

56. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

57. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

58. Defendants thus infringe one or more claims of the 802 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 802 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 802 Patents.

59. Broadway has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

60. Broadway has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 802 Patent by others and Broadway will continue to do so unless enjoined by this Court. Broadway's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to,

encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 802 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Broadway knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 802 Patent.

61. Broadway continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 802 Patent.

62. Broadway has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 802 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

63. Broadway has committed these acts of infringement without license or authorization.

64. By engaging in the conduct described herein, Broadway has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Broadway is thus liable to Textile for infringement of the 802 Patent, pursuant to 35 U.S.C. § 271.

65. As a direct and proximate result of Broadway's infringement of the 802 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Broadway's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

66. In addition, the infringing acts and practices of Broadway have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Broadway is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Broadway is finally and permanently enjoined from further infringement.

67. Broadway has had actual knowledge of the 802 Patent at least as of October 18, 2013, when Textile sent a letter to James D. Goudge, then Chief Executive Officer of Broadway Bank, that described certain implementations of the patented technology and specifically identified the 802 Patent.

68. Broadway has had actual knowledge of the 802 Patent at least as of October 25, 2013, when Textile sent a letter to Jeff Foote, then Executive Vice President of Broadway Bank,

that described certain implementations of the patented technology and specifically identified the 802 Patent.

69. Broadway has had actual knowledge of the 802 Patent at least as of November 10, 2014, when Textile sent two letters – one to James D. Goudge, then Chief Executive Officer of Broadway Bank, and one to Jeff Foote, then Executive Vice President of Broadway Bank, that described certain implementations of the patented technology and specifically identified the 802 Patent.

70. Broadway has had actual knowledge of the 802 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Broadway will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 802 Patent.

71. Broadway has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 802 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

72. Textile has been damaged as a result of the infringing conduct by Broadway alleged above. Thus, Broadway is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

73. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 802 Patent.

COUNT III

INFRINGEMENT OF U.S. PATENT NO. 9,584,499

74. On February 28, 2017, United States Patent No. 9,584,499 (“the 499 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

75. Textile is the owner of the 499 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 499 Patent against infringers, and to collect damages for all relevant times.

76. Broadway offers debit and/or credit cards, such as the Broadway Bank Visa Contactless Debit Card, that are used by Broadway in practicing a method for authorizing transaction specific access to a secured resource having a secured resource identity (the “Accused Instrumentality”). The Broadway transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.



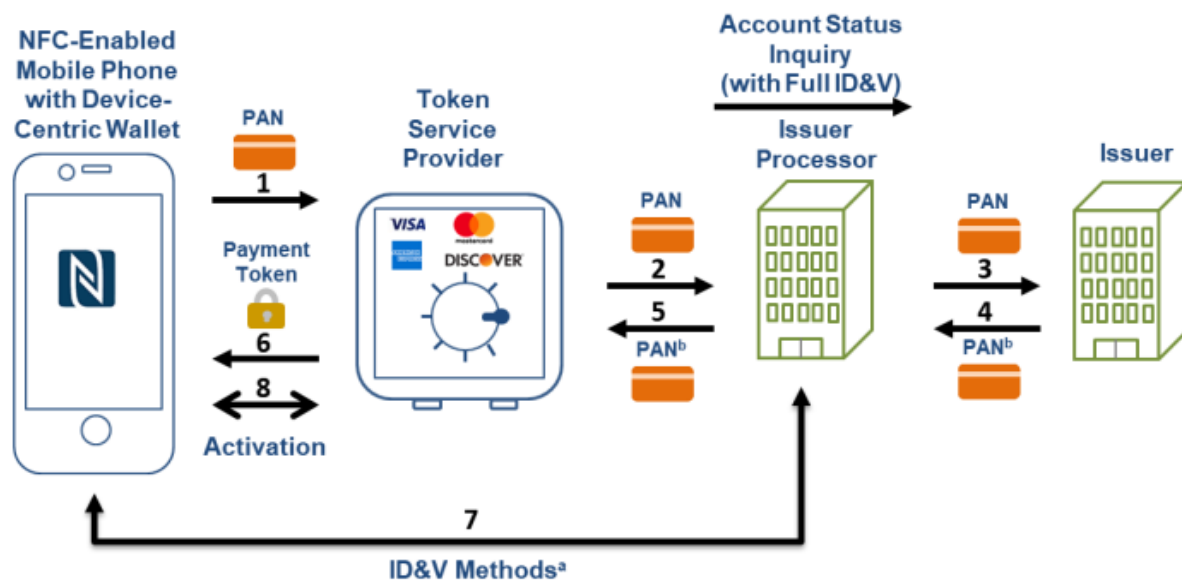
Pay with Your Hand-held Device

Your Broadway Bank Visa® Debit card is digital wallet ready. Digital wallets are a great way to virtually load a physical card into a mobile app and store it for fast, easy access at the point of sale. You can use this feature with Apple Pay®, Google Pay® and Samsung Pay®.

(Source: <https://broadway.bank/personal/checking-savings/tools/debit-card>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^a ID&V methods includes text or email or call. OTP is an example.

^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

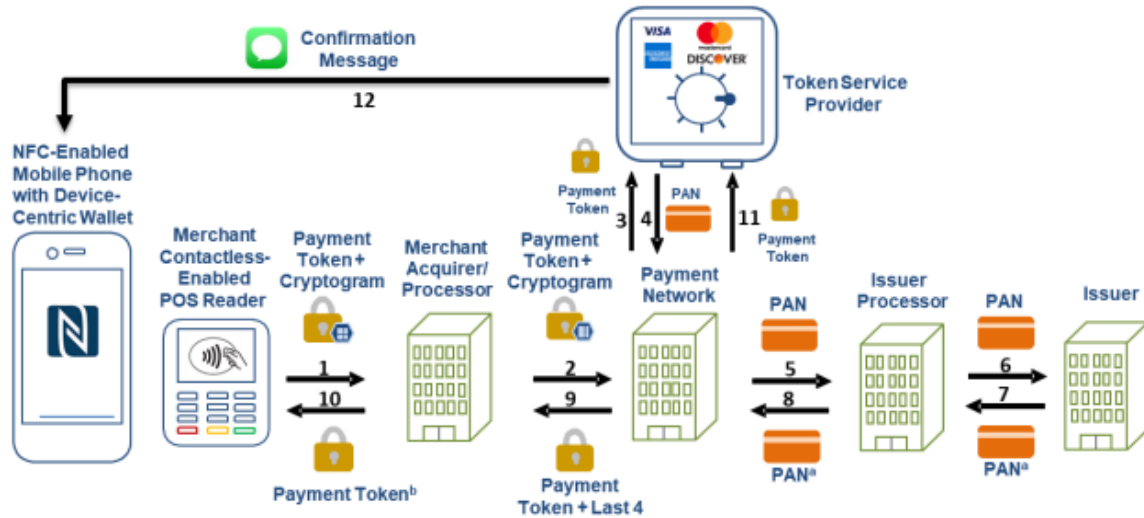
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

77. Broadway's use of the Accused Instrumentality includes a method for authorizing transaction specific access to a secured resource having a secured resource identity. For example, a Broadway account holder requests Broadway to provision a specific Broadway debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Broadway card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's

smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram.

78. The Accused Instrumentality includes receiving at a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive a request for transaction specific access to a secured resource by a service client. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Broadway card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Broadway card account of the account holder. This messaging gateway is either hosted directly by Broadway or through an agent with whom Broadway has contracted to receive the messages.

79. The Accused Instrumentality includes generating a key string with a server in communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate the key string known to both said server and an authorized user of the secured resource, said key string being associated with the secured resource within a key string table accessible by the server and providing a basis for authenticating the secured resource identity by searching the key string table for the key string. For example, behind the firewall of the messaging gateway and in communication therewith is an authorization server that generates a token corresponding to a secured resource during the

provisioning process. After this, the authorization server updates a table that maps token numbers to secured resource identities. The authorization server is then able to search the table to authenticate a secured resource identity by searching the table for the token. If the token has a corresponding secured resource identity, that identity is authenticated. The authorization server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to provide the authentication services.

80. The Accused Instrumentality includes determining transaction specific information with the server in communication with the messaging gateway, the server having a third set of instructions embodied in a computer readable medium operable to identify transaction specific information within the request. For example, the authorization server is also programmed to identify within the payment authorization request transaction specific information that was passed by the merchant. The authorization server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to provide the authentication services.

81. The Accused Instrumentality includes communicating said key string to said authorized user. For example, once the provisioning process is complete, the messaging gateway and/or the server send the token to the authorized user's mobile device. The messaging gateway is either hosted directly by Broadway or through an agent with whom Broadway has contracted to provide the authentication services. The authorization server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to provide the authentication services.

82. The Accused Instrumentality includes receiving an authentication credential from said service client, said authentication credential having been provided to said service client by

said authorized user. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant. The authorization server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to provide the authentication services.

83. The Accused Instrumentality includes evaluating said authentication credential. For example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authorizes the transaction specific access. The authorization server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to provide the authentication services.

84. The Accused Instrumentality includes wherein the key string and authentication credential do not reveal any primary identifier associated with said secured resource. For example, neither the token nor the cryptogram reveals the debit and/or credit card number associated with the secured resource.

85. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

86. Defendants thus infringe one or more claims of the 499 Patent. The elements and conduct described herein are covered by and infringe upon at least Claim 3 of the 499 Patent.

Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 499 Patent.

87. Broadway has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

88. Broadway has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 499 Patent by others and Broadway will continue to do so unless enjoined by this Court. Broadway's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 499 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Broadway knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 499 Patent.

89. Broadway continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers,

businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 499 Patent.

90. Broadway has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 499 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

91. Broadway has committed these acts of infringement without license or authorization.

92. By engaging in the conduct described herein, Broadway has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Broadway is thus liable to Textile for infringement of the 499 Patent, pursuant to 35 U.S.C. § 271.

93. As a direct and proximate result of Broadway's infringement of the 499 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Broadway's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

94. In addition, the infringing acts and practices of Broadway have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Broadway is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Broadway is finally and permanently enjoined from further infringement.

95. Broadway has had actual knowledge of the 499 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Broadway will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 499 Patent.

96. Broadway has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 499 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

97. Textile has been damaged as a result of the infringing conduct by Broadway alleged above. Thus, Broadway is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

98. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 499 Patent.

COUNT IV

INFRINGEMENT OF U.S. PATENT NO. 10,148,659

99. On December 4, 2018, United States Patent No. 10,148,659 (“the 659 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

100. Textile is the owner of the 659 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 659 Patent against infringers, and to collect damages for all relevant times.

101. Broadway offers debit and/or credit cards, such as the Broadway Bank Visa Contactless Debit Card, that are used with a computer-implemented system for a credit or debit and/or credit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit and/or credit card account number to the merchant (the “Accused Instrumentality”). The Broadway transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.



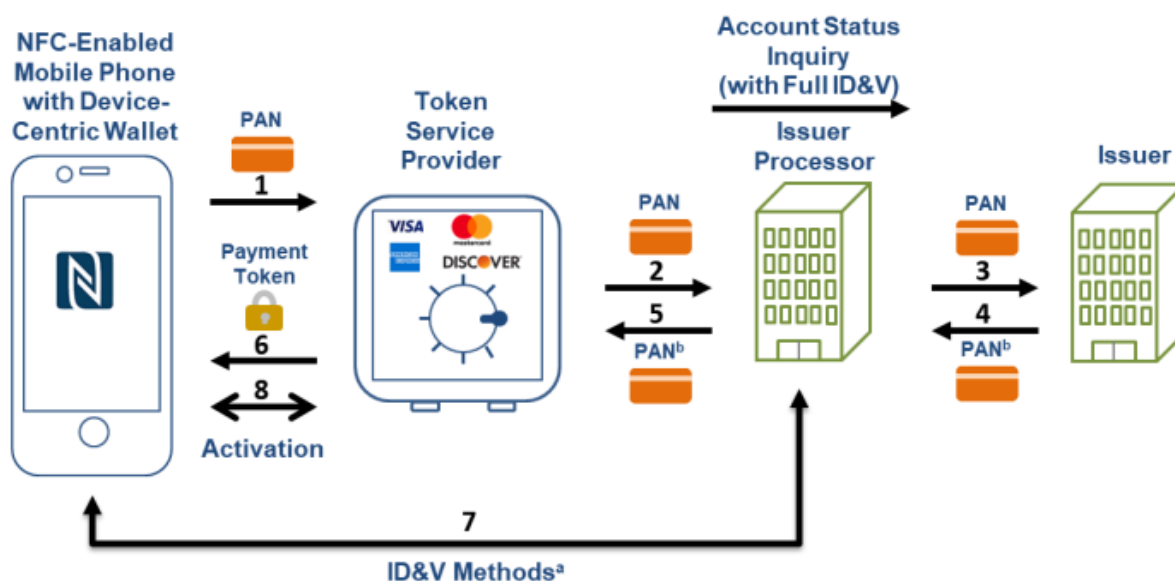
Pay with Your Hand-held Device

Your Broadway Bank Visa® Debit card is digital wallet ready. Digital wallets are a great way to virtually load a physical card into a mobile app and store it for fast, easy access at the point of sale. You can use this feature with Apple Pay®, Google Pay® and Samsung Pay®.

(Source: <https://broadway.bank/personal/checking-savings/tools/debit-card>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^a ID&V methods includes text or email or call. OTP is an example.

^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

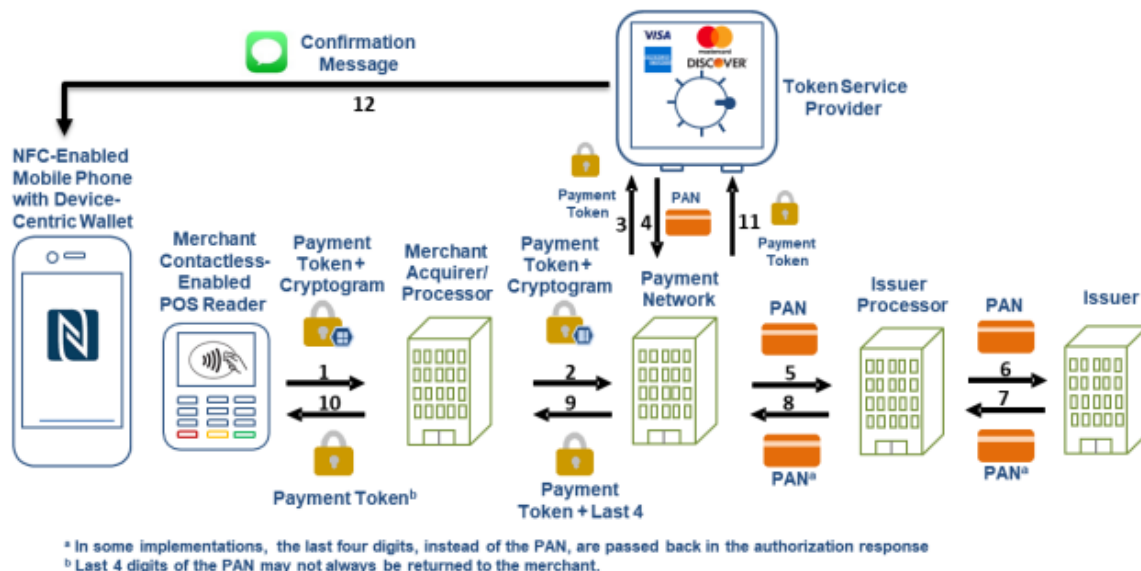


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

102. The Accused Instrumentality includes a computer-implemented system for a credit or debit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit card account number to the merchant. For example, a Broadway account holder requests Broadway to provision a specific Broadway debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Broadway to a specific merchant in a specific amount for a specific transaction from a specific

Broadway card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

103. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a credit or debit card account holder's mobile device, a merchant's payment application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a Broadway card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Broadway card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Broadway card account of the account holder. This interface is either hosted directly by Broadway or through an agent with whom Broadway has contracted to receive the messages.

104. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration

information received from the credit or debit card account holder through the at least one interface, the registration information comprising a credit or debit card account holder identifier and at least one credit or debit card account number having an associated unique account identifier wherein the credit or debit card account number and unique account identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card and the debit and/or credit card account number (which has a corresponding token), received from Broadway card account holders through the interface for provisioning a specific Broadway debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Broadway card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Broadway card account of the account holder. The server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to receive the messages.

105. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to pay the specific merchant for the specific transaction from a given debit or credit card account, the authorization request message having been received through the at least one interface and originating from the credit or debit card account holder's mobile device and comprising: a first merchant identifier; a first transaction specific information selected from the group consisting of a first transaction amount and first client reference identifier; the credit or debit card account holder identifier; and a designated unique account identifier selected from the at least one unique account identifiers. For example, the Accused

Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Broadway card account holder's mobile device. The server is programmed to receive authorization requests initiated by Broadway card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a merchant identifier, and the Broadway card account holder identifier. The server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to receive the messages.

106. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string wherein the key string is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the designated unique account identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to receive the messages.

107. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive a payment request message from the merchant's payment application through the at least one interface, the payment request message comprising: a second merchant identifier; a second transaction specific information selected from the group consisting of a second transaction amount and second client reference identifier; and a second transaction specific authentication credential whereby the second authentication credential was received by the merchant application from the credit or debit card account holder's mobile device. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Broadway card account holder's mobile device. The server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to receive the messages.

108. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the credit or debit card account holder's request to use the credit or debit card account number associated with the designated unique account identifier for payment to the specific merchant for the specific transaction and authorizing the resource provider to use the credit or debit card account number associated with the designated unique account identifier to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or bank account number to the

specific merchant by determining if: the first merchant identifier matches the second merchant identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to provide the authentication services.

109. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

110. Defendants thus infringe one or more claims of the 659 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 9 of the 659 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 659 Patent.

111. Broadway has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C.

§ 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

112. Broadway has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 659 Patent by others and Broadway will continue to do so unless enjoined by this Court. Broadway's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 659 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Broadway knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 659 Patent.

113. Broadway continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 659 Patent.

114. Broadway has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 9 of the 659 Patent, in violation of 35 U.S.C.

§ 271(c), by contributing to the direct infringement of the 659 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

115. Broadway has committed these acts of infringement without license or authorization.

116. By engaging in the conduct described herein, Broadway has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Broadway is thus liable to Textile for infringement of the 659 Patent, pursuant to 35 U.S.C. § 271.

117. As a direct and proximate result of Broadway's infringement of the 659 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Broadway's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

118. In addition, the infringing acts and practices of Broadway have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Broadway is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As

such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Broadway is finally and permanently enjoined from further infringement.

119. Broadway has had actual knowledge of the 659 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Broadway will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 659 Patent.

120. Broadway has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 659 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

121. Textile has been damaged as a result of the infringing conduct by Broadway alleged above. Thus, Broadway is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

122. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 659 Patent.

COUNT V

INFRINGEMENT OF U.S. PATENT NO. 10,560,454

123. On February 11, 2020, United States Patent No. 10,560,454 (“the 454 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

124. Textile is the owner of the 454 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 454 Patent against infringers, and to collect damages for all relevant times.

125. Broadway offers debit and/or credit cards, such as the Broadway Bank Visa Contactless Debit Card, that are used with a computer-implemented system for a user to authorize a resource authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client (the "Accused Instrumentality"). The Broadway transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



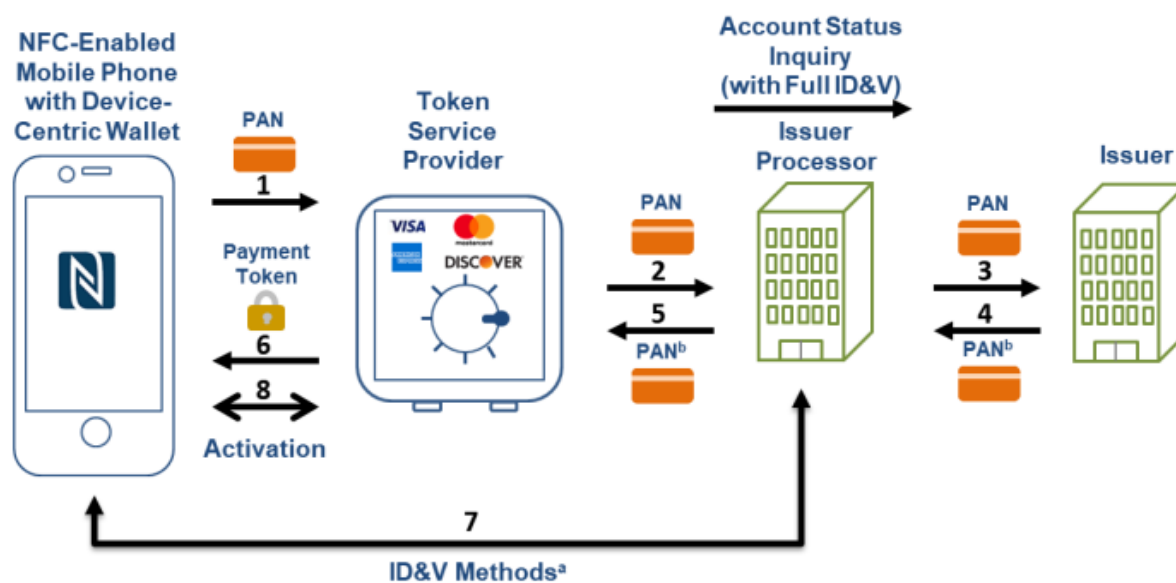
Pay with Your Hand-held Device

Your Broadway Bank Visa® Debit card is digital wallet ready. Digital wallets are a great way to virtually load a physical card into a mobile app and store it for fast, easy access at the point of sale. You can use this feature with Apple Pay®, Google Pay® and Samsung Pay®.

(Source: <https://broadway.bank/personal/checking-savings/tools/debit-card>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^a ID&V methods includes text or email or call. OTP is an example.

^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

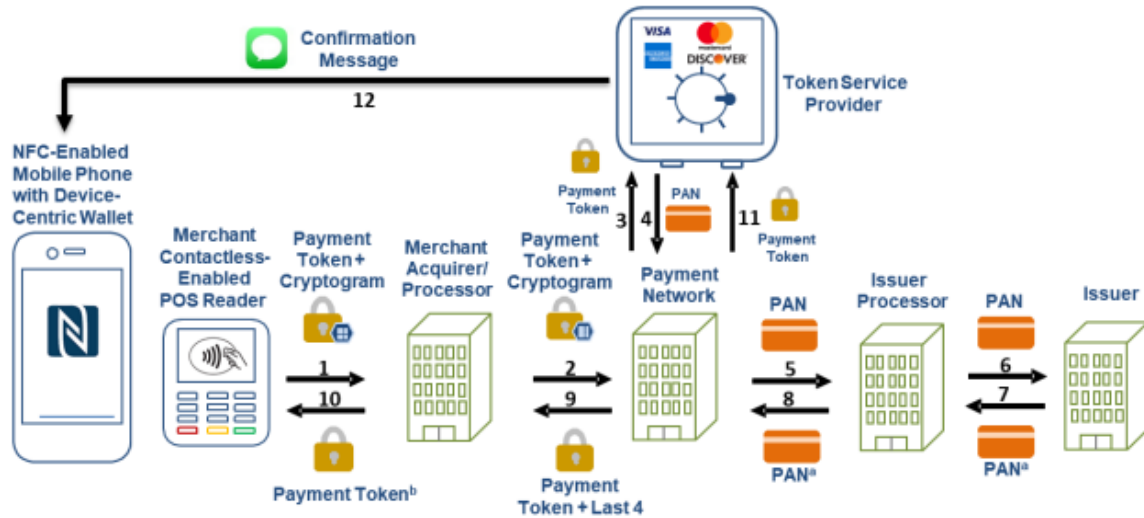
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

126. The Accused Instrumentality includes a computer-implemented system for a user to authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client. For example, a Broadway account holder requests Broadway to provision a specific Broadway debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Broadway to a specific merchant in a specific amount for a specific transaction from a specific Broadway card account of the account holder

using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

127. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a user's application, a service client's application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a Broadway card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Broadway card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Broadway card account of the account holder. This interface is either hosted directly by Broadway or through an agent with whom Broadway has contracted to receive the messages.

128. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration information received from the user through the at least one interface, the registration information comprising a user identifier and at least one secured resource identifier associated with the

common identifier of the secured resource, wherein the common identifier and secured resource identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card, the debit and/or credit card account number (which has a corresponding token), and the CVV number received from Broadway card account holders through the interface for provisioning a specific Broadway debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Broadway card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Broadway card account of the account holder. The server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to receive the messages.

129. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to authorize access to the secured resource by the service client, the authorization request message having been received through the at least one interface from the user's application and comprising: a first service client identifier; a first transaction specific information; the user identifier; and a designated secured resource identifier selected from one of the at least one secured resource identifiers. For example, the Accused Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Broadway card account holder's mobile device. The server is programmed to receive authorization requests initiated by Broadway card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction,

a token, a CVV number, a merchant identifier, other token information, and the Broadway card account holder identifier. The server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to receive the messages.

130. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string and does not include or reveal the common identifier associated with the designated secured resource identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to receive the messages.

131. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive an access request message from the service client's application through the at least one interface, the payment request message comprising: a second service client identifier; a second transaction specific information; and a second transaction specific authentication credential whereby the second transaction specific authentication credential was received by the service client's

application from the user's application. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Broadway card account holder's mobile device. The server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to receive the messages.

132. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the user's request to access the secured resource associated with the designated secured resource identifier without transmitting or otherwise providing the common identifier of the secured resource to the service client by determining if: the first service client identifier matches the second service client identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Broadway or through an agent with whom Broadway has contracted to provide the authentication services.

133. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

134. Defendants thus infringe one or more claims of the 454 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 8 of the 454 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 454 Patent.

135. Broadway has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

136. Broadway has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 454 Patent by others and Broadway will continue to do so unless enjoined by this Court. Broadway's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for

another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 454 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Broadway knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 454 Patent.

137. Broadway continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 454 Patent.

138. Broadway has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 454 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

139. Broadway has committed these acts of infringement without license or authorization.

140. By engaging in the conduct described herein, Broadway has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Broadway is thus liable to Textile for infringement of the 454 Patent, pursuant to 35 U.S.C. § 271.

141. As a direct and proximate result of Broadway's infringement of the 454 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Broadway's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

142. In addition, the infringing acts and practices of Broadway have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Broadway is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Broadway is finally and permanently enjoined from further infringement.

143. Broadway has had actual knowledge of the 454 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Broadway will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 454 Patent.

144. Broadway has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 454 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

145. Textile has been damaged as a result of the infringing conduct by Broadway alleged above. Thus, Broadway is liable to Textile in an amount that adequately compensates it

for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

146. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 454 Patent.

ADDITIONAL ALLEGATIONS REGARDING INFRINGEMENT

147. Broadway has also indirectly infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by inducing others to directly infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Broadway has induced the end-users, Broadway's customers, to directly infringe (literally and/or under the doctrine of equivalents) the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by using the Accused Instrumentality.

148. Broadway took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

149. Such steps by Broadway included, among other things, advising or directing customers and end-users to use the Accused Instrumentality in an infringing manner; advertising and promoting the use of the Accused Instrumentality in an infringing manner; and/or distributing instructions that guide users to use the Accused Instrumentality in an infringing manner.

150. Broadway has performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454

Patent and with the knowledge that the induced acts constitute infringement, at least since the filing of the Complaint.

151. Broadway was and is aware that the normal and customary use of the Accused Instrumentality by Broadway's customers would infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Broadway's inducement is ongoing.

152. Broadway directs or controls the use of the Accused Instrumentality nationwide through its own websites and in its own branches, including in Texas and elsewhere in the United States, and expects and intends that the Accused Instrumentality will be so used.

153. Broadway took active steps, directly and/or through contractual relationships with others, with the specific intent to cause such persons to make or use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

154. Broadway performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts would constitute infringement.

155. Broadway's inducement is ongoing.

156. Broadway has also indirectly infringed by contributing to the infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Broadway has contributed to the direct infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by the end-user of the Accused Instrumentality.

157. The Accused Instrumentality has special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the 079

Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

158. As described above, the special features include securely authorizing specific transactions without providing a credit or debit card number to the merchant used in a manner that infringes the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

159. The special features constitute a material part of the invention of one or more of the claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and are not staple articles of commerce suitable for substantial non-infringing use.

160. Broadway's contributory infringement is ongoing.

161. Broadway's actions are at least objectively reckless as to the risk of infringing valid patents and this objective risk was either known or should have been known by Broadway, at least since the filing of the Complaint.

162. Broadway has had knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent at least since the filing of the Complaint.

163. Broadway's customers have infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

164. Broadway encouraged its customers' infringement.

165. Broadway's direct and indirect infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent is, has been, and/or continues to be willful, intentional, deliberate, and/or in conscious disregard of Textile's rights under the patents.

166. Textile has been damaged as a result of the infringing conduct by Broadway alleged above. Thus, Broadway is liable to Textile in an amount that adequately compensates it

for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Textile hereby requests a trial by jury on all issues so triable by right.

PRAYER FOR RELIEF

Textile requests that the Court find in its favor and against Broadway, and that the Court grant Textile the following relief:

- a. Judgment that one or more claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent have been infringed, either literally and/or under the doctrine of equivalents, by Broadway and/or all others acting in concert therewith;
- b. A permanent injunction enjoining Broadway and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert therewith from infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent; or, in the alternative, an award of a reasonable ongoing royalty for future infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by such entities;
- c. Judgment that Broadway account for and pay to Textile all damages to and costs incurred by Textile because of Broadway's infringing activities and other conduct complained of herein, including an award of all increased damages to which Textile is entitled under 35 U.S.C. § 284;
- d. That Textile be granted pre-judgment and post-judgment interest on the damages caused by Broadway's infringing activities and other conduct complained of herein;
- e. That this Court declare this an exceptional case and award Textile its reasonable

attorney's fees and costs in accordance with 35 U.S.C. § 285; and

f. That Textile be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: October 12, 2021

Respectfully submitted,

/s/ Matthew J. Antonelli

Matthew J. Antonelli

Texas Bar No. 24068432

matt@ahtlawfirm.com

Zachariah S. Harrington

Texas Bar No. 24057886

zac@ahtlawfirm.com

Larry D. Thompson, Jr.

Texas Bar No. 24051428

larry@ahtlawfirm.com

Christopher Ryan Pinckney

Texas Bar No. 24067819

ryan@ahtlawfirm.com

ANTONELLI, HARRINGTON

& THOMPSON LLP

4306 Yoakum Blvd., Ste. 450

Houston, TX 77006

(713) 581-3000

Stafford Davis

State Bar No. 24054605

sdavis@stafforddavisfirm.com

Catherine Bartles

Texas Bar No. 24104849

cbartles@stafforddavisfirm.com

THE STAFFORD DAVIS FIRM

815 South Broadway Avenue

Tyler, Texas 75701

(903) 593-7000

(903) 705-7369 fax

Of Counsel:

Sandeep Seth

Texas State Bar No. 18043000

SETHLAW

Pennzoil Place

700 Milam Street, Suite 1300

Houston, Texas 77002
Telephone: (713) 244-5017
ss@sethlaw.com

Attorneys for Textile Computer Systems, Inc.

EXHIBIT 2B

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

TEXTILE COMPUTER SYSTEMS, INC.,

Plaintiff,

v.

CHARLES SCHWAB BANK,

Defendant.

CIVIL ACTION NO. 6:21-cv-1051

ORIGINAL COMPLAINT FOR
PATENT INFRINGEMENT

JURY TRIAL DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Textile Computer Systems, Inc. (“Textile” or “Plaintiff”) files this original complaint against Defendant Charles Schwab Bank (“Charles Schwab”), alleging, based on its own knowledge as to itself and its own actions and based on information and belief as to all other matters, as follows:

PARTIES

1. Textile Computer Systems, Inc. is a corporation formed under the laws of the State of Texas, with a place of business at 618 Bluff Trail, San Antonio, Texas, 78216.

2. Charles Schwab Bank is a federally chartered savings association with its headquarters in Texas and with places of business in Austin, Texas, El Paso, Texas, and San Antonio, Texas.

3. Charles Schwab and its affiliates lead and are part of an interrelated group of companies which together comprise one of the country’s largest banking and financial service entities, including under the Charles Schwab brand.

4. Charles Schwab and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

5. Charles Schwab and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

6. Charles Schwab and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

7. Thus, Charles Schwab and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

JURISDICTION AND VENUE

8. This is an action for infringement of United States patents arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. § 1331 and § 1338(a).

9. This Court has personal jurisdiction over Charles Schwab pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Charles Schwab has done and continues to do business in Texas; and (ii) Charles Schwab has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations, inducing others to commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein.

10. Venue is proper in this district pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Charles Schwab has committed and continues to commit acts of patent infringement in this district. For example, Charles Schwab cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those cardholders make and/or use the accused instrumentalities in the district. Charles Schwab induces others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. Charles Schwab has regular and established places of business in this district, including at least at its El Paso Operation Center at 1945 Northwestern Drive, El Paso, Texas 79912, its branch at 1435 North Loop 1604 West, Suite 101, San Antonio, Texas 78258, and at numerous other locations in San Antonio and Austin:

U.S. Mailing Address

Standard Mailing Address

Charles Schwab & Co., Inc.
El Paso Operation Center
P.O. Box 982600
El Paso, TX 79998

Overnight Mailing Address

Charles Schwab & Co., Inc.
El Paso Operation Center
1945 Northwestern Drive
El Paso, TX 79912

U.S. Mailing Address

Standard Mailing Address

Charles Schwab & Co., Inc.
Orlando Operations Center
P.O. Box 628291
Orlando, FL 32862-8291

Overnight Mailing Address

Charles Schwab & Co., Inc.
Orlando Operations Center
1958 Summit Park Drive, Suite 200
Orlando, FL 32810

International Mailing Address

Regular Mail:

Charles Schwab & Co., Inc.
Attn: Global Operations
PO Box 2912
Phoenix, AZ 85062-2912
USA

Overnight/Express Mail:

Charles Schwab & Co., Inc.
Attn: Phoenix ROC Document Control (Global Operations)
2423 E. Lincoln Drive
Phoenix, AZ 85016
USA

Brokerage Services

- TeleBroker® **800-272-4922**
[Learn more about TeleBroker >](#)
- Schwab 529 **888-903-3863**
Monday-Friday, 6:30 a.m.-3:30 p.m. PT
- Via TTY services for the hearing impaired
800-345-2550

Multilingual and International Services

- Mandarin or Cantonese **800-662-6068**
[Learn more about our Mandarin and Cantonese services 中文 >](#)
From outside the United States **+1-415-667-8400**
- Vietnamese **866-824-8438**
From inside the United States **877-853-1802**
- Spanish **800-786-5174**

Lost or Stolen Card

- Report a lost or stolen Schwab One® Visa® Platinum Debit Card
800-421-4488
24/7 access
- From outside the United States
+1-317-596-4501

Schwab Bank Automated Services



877-824-5625
24/7 access

Schwab Bank Lost, Damaged, or Stolen Card

Replace a lost or damaged Schwab Bank Visa® Platinum Debit Card on Schwab.com.

[Replace a debit card](#) ↗

Report a stolen Schwab Bank Visa® Platinum Debit Card
888-403-9000
24/7 access

From outside the United States
+1-317-596-4501

Mortgage Customers

If you'd like to send a qualified written request, notice of error, or information request, please see your monthly statement for the address of your loan servicer. If you have questions about your loan, please contact the phone number listed on your monthly statement.

(Source: <https://www.schwab.com/contact-us>)



(Source: screenshot from Google Maps Street View)

Charles Schwab

Find a Branch | Find a Consultant

What We Offer | What We Charge | Why Schwab | Insights

Open an Account

A relationship you can trust, close to home.

Schwab Branch, San Antonio

1435 North Loop 1604 West, Suite 101
San Antonio, TX 78258

Hours today: 8:30 a.m. - 5:00 p.m.

Branch phone: 210-832-2300

For support 24/7: 800-435-4000

Directions and parking

Check deposits accepted until 5:00 p.m.
Cash deposits are not accepted.

Directions | Appointments | Consultants | Chat

(Source: <https://client.schwab.com/public/branchlocator/branchdetails.aspx?branchid=1225>)



(Source: screenshot from Google Maps Street View)

BACKGROUND

11. The patents-in-suit generally pertain to payment authorization technology used in payment networks used to process transactions from, for example, credit cards and debit cards. The technology disclosed by the patents was developed by Gopal Nandakumar, a Texas-based entrepreneur, software engineer, and prolific inventor with over 30 years of experience in the field of Information Management Systems.

12. In 1987, after receiving Master's Degrees from both the University of Madras, India and the Georgia Institute of Technology, Mr. Nandakumar formed Textile Computer Systems, Inc. ("Textile") for the purpose of consulting and developing software for the textile industry. In 2005, Textile began transitioning into credit card transaction systems. In 2011, Textile began to develop and market the MySingleLink suite of applications.

13. The Nandakumar patents are related to payment authorization technology. Mr. Nandakumar has been at the forefront of payment authorization, developing, disclosing, and patenting solutions for reducing fraud in credit and debit card transactions. Indeed, the

Nandakumar patents (or the applications leading to them) have been cited during patent prosecution over a hundred times, including by numerous leading companies in the payment authorization industry such as ADP, Bank of America, Google, Groupon, IBM, Mastercard, NEC, Paypal, Visa, and Wells Fargo.

THE TECHNOLOGY

14. The patents-in-suit, U.S. Patent Nos. 8,505,079, 8,533,802, 9,584,499, 10,148,659, and 10,560,454 (collectively, the “Asserted Patents”), teach systems, including payment processing systems, for securely and effectively approving and processing specific credit card and/or debit card transactions. Through the specific use of servers, messaging gateways, and/or interfaces, these systems act to reduce credit card and/or debit card fraud and misuse through their use and validation of key strings, authentication credentials, transaction specific information, and transaction specific credentials. The technology in the Asserted Patents improves the underlying functionality of existing card processing infrastructure by minimizing fraud and data theft in the face of attacks on payment systems that continue to grow in their number and sophistication.

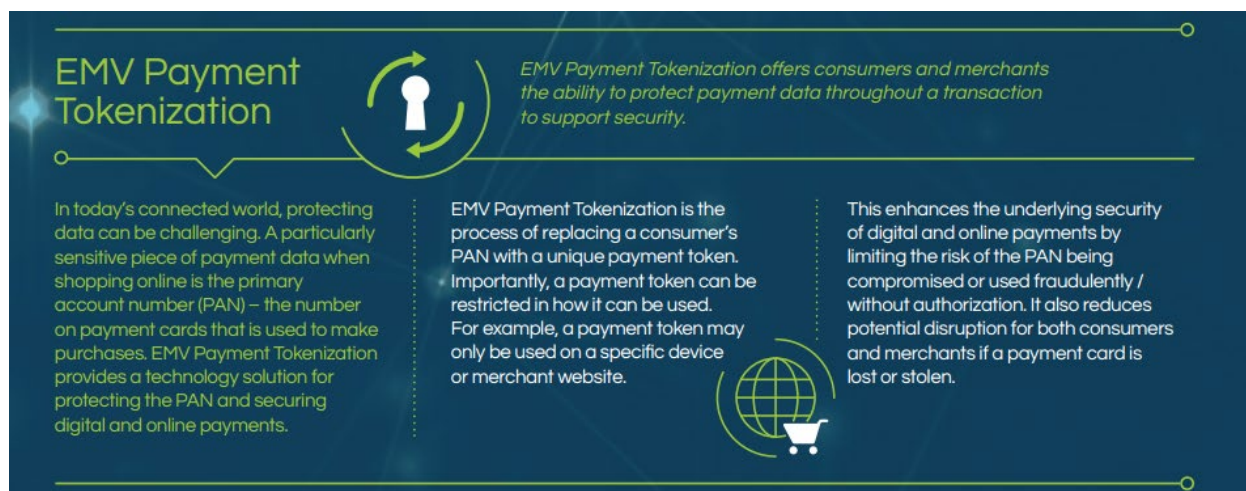
15. The patented improvements are critical for implementing secure payment systems, especially in light of the many high-profile merchant data breaches that have lead to increased credit and debit card fraud. For example, in 2006, TJX Companies, who owns retailers like TJMaxx and Marshall’s, was hit with a cyber attack that resulted in the theft of credit cards leading to over \$100 million in fraud losses. In 2013, five people were indicted for attacking a number of retailers and financial institutions including NASDAQ, 7-Eleven, JCP, and others, stealing over 160 million cards. Also in 2013, the retailer Target suffered a data breach that resulted in 40 million debit and credit cards being compromised.

16. One implementation of the technology claimed in the Asserted Patents has been described by EMVCo as “a global Payment Tokenisation ecosystem that overlays and interoperates with existing payment ecosystems to support digital commerce and new methods of payment” and as “enhanc[ing] the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorized or fraudulent use of PANs.”

(Source: <https://www.emvco.com/emv-technologies/payment-tokenisation/>).

17. The technology claimed in the Asserted Patents is far from conventional technology. The payment industry gathered and consulted experts who worked together over a number of years to develop infringing payment tokenisation systems. In other words, the technology claimed in the Asserted Patents was not existing or conventional technology that the payment industry had sitting on the shelf.

18. Indeed, as recently as February of this year, EMVCo itself recognized that an implementation of the technology claimed in the Asserted Patents “provides a technology solution for protecting the PAN and securing digital and online payments”:



(Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

19. That same EMVCo document notes that “In today’s connected world, protecting data can be challenging. A particularly sensitive piece of payment data when shopping online is the primary account number (PAN) – the number on payment cards that is used to make purchases” and that EMVCo’s payment tokenization “enhances the underlying security of digital and online payments by limiting the risk of the PAN being compromised or used fraudulently / without authorization.” The document also states that the “Payment Tokenisation Specification provides an interoperable Technical Framework.” (Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

20. One of the asserted patents, the 079 Patent, was challenged in an Inter Partes Review proceeding before the Patent and Trademark Office (“PTO”). The PTO found that the challenger, Unified Patents Inc., was unable to show that one element, the “key string” as claimed in the 079 Patent claims and as construed by the PTO, was in the prior art at all, much less it being conventional or widespread. The PTO thus confirmed the patentability of all challenged claims of the 079 Patent.

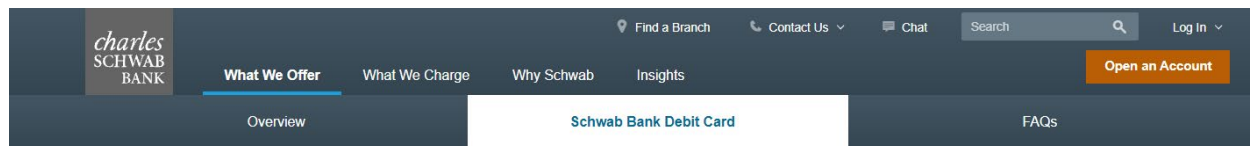
COUNT I

INFRINGEMENT OF U.S. PATENT NO. 8,505,079

21. On August 6, 2013, United States Patent No. 8,505,079 (“the 079 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

22. Textile is the owner of the 079 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 079 Patent against infringers, and to collect damages for all relevant times.

23. Charles Schwab offers debit and/or credit cards, such as the Schwab Bank Visa Platinum Debit Cards, that are used with an authentication system that authenticates the identity of a Charles Schwab card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Charles Schwab card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities, for example. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.



Make the most of your
Schwab Bank Visa®
Platinum Debit Card.

[Open a Checking Account](#)



Contactless.

Pay securely and without making contact. All you have to do is tap and hold your Schwab Bank Visa Platinum Debit Card at a contactless-enabled terminal. Each transaction is accompanied by a one-time code so no personal information is exchanged. You can still insert or swipe your card if contactless isn't available. It's easy, convenient, and safe.

[Contactless FAQs >](#)



Make your phone your new
wallet.

Add your Schwab Bank Visa Platinum Debit Card to your mobile wallet¹ for a more secure, convenient, and easy way to pay. At checkout, just click, glance, or touch and hold your device near the reader to pay. It's safe, secure, and simple.

[Mobile wallet FAQs >](#)



1

Open the app.

Download or locate the mobile wallet app (it is most likely already loaded on your smart device).

2

Add your card.

Add your Schwab Bank Visa Platinum Debit Card information to the mobile wallet.

3

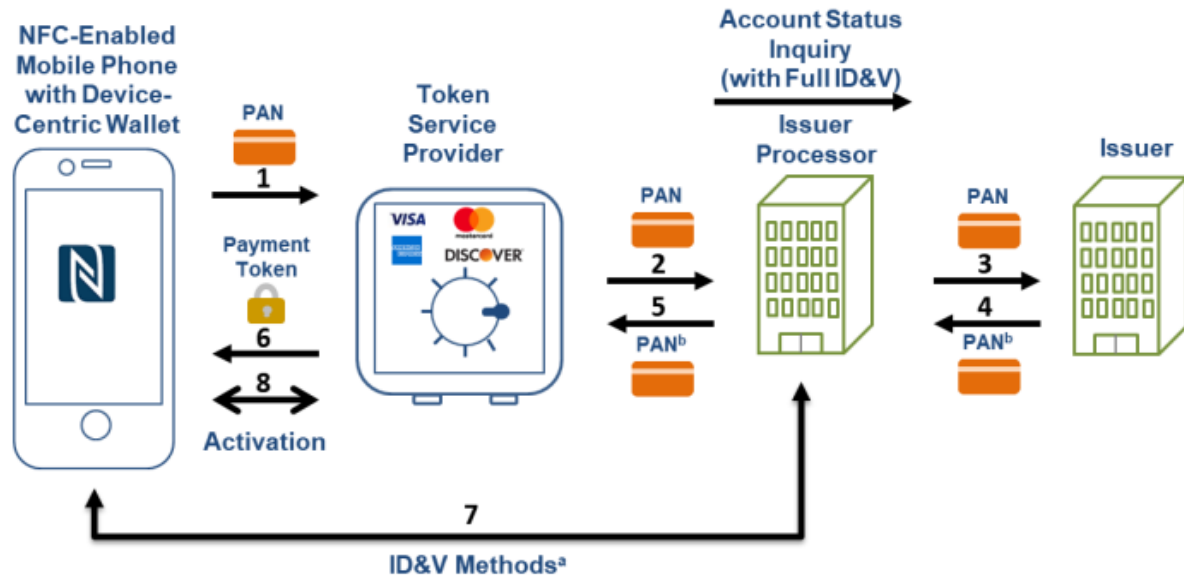
Prepare to shop.

When you check out at participating merchants, access your debit card and just click, glance, or touch and hold your device near the reader to pay. It's safe, secure and simple.

(Source: <https://www.schwab.com/checking/debit-card>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^a ID&V methods includes text or email or call. OTP is an example.

^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

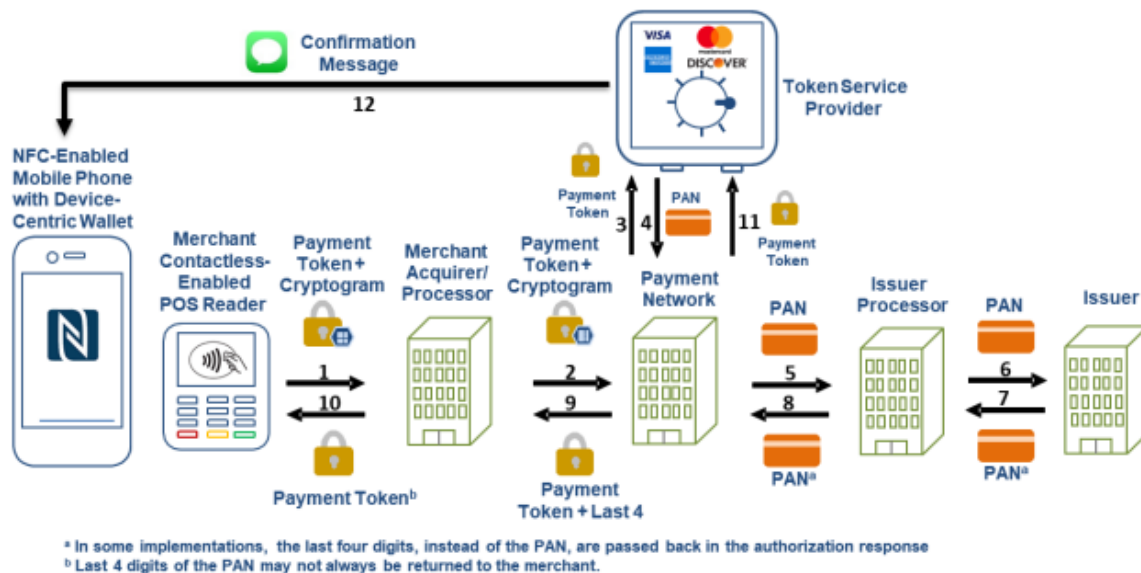


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

24. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a Charles Schwab account holder requests Charles Schwab to provision a specific Charles Schwab debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Charles Schwab card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the

request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

25. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Charles Schwab card account holders for provisioning a specific Charles Schwab debit and/or credit card for use on their mobile devices. The messaging gateway is also programmed to receive requests initiated by Charles Schwab card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Charles Schwab card account of the account holder. This messaging gateway is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to receive the messages.

26. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to determine a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the messaging

gateway and in secure communication therewith is an authorization server that processes the received request to identify the token value sent for the account selected to be charged that was passed from the authorized user to the merchant terminal via the NFC communication link. From the token value, the server can look up the debit and/or credit card account number. The authorization server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to provide the authentication services.

27. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive within the payment authorization request transaction specific information that was input into the request by the merchant. The interface is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to provide the authentication services.

28. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

29. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For

example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

30. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

31. Defendants thus infringe one or more of the claims of the 079 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 079 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 079 Patent.

32. Charles Schwab has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(a), by making, using, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

33. Charles Schwab has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 079 Patent by others and Charles Schwab will continue to do so unless enjoined by this Court. Charles Schwab's deliberate and/or willfully blind actions include, but are not limited to, actively

marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 079 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Charles Schwab knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 079 Patent.

34. Charles Schwab continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 079 Patent.

35. Charles Schwab has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 079 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for

use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

36. Charles Schwab has committed these acts of infringement without license or authorization.

37. By engaging in the conduct described herein, Charles Schwab has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Charles Schwab is thus liable to Textile for infringement of the 079 Patent, pursuant to 35 U.S.C. § 271.

38. As a direct and proximate result of Charles Schwab's infringement of the 079 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Charles Schwab's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

39. In addition, the infringing acts and practices of Charles Schwab have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Charles Schwab is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Charles Schwab is finally and permanently enjoined from further infringement.

40. Charles Schwab has had actual knowledge of the 079 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Charles Schwab will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 079 Patent.

41. Charles Schwab has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 079 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

42. Textile has been damaged as a result of the infringing conduct by Charles Schwab alleged above. Thus, Charles Schwab is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

43. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 079 Patent.

COUNT II

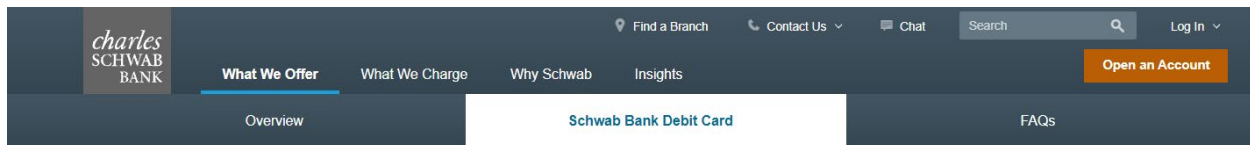
INFRINGEMENT OF U.S. PATENT NO. 8,533,802

44. On September 10, 2013, United States Patent No. 8,533,802 (“the 802 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

45. Textile is the owner of the 802 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 802 Patent against infringers, and to collect damages for all relevant times.

46. Charles Schwab offers debit and/or credit cards, such as the Schwab Bank Visa Platinum Debit Cards, that are used with an authentication system that authenticates the identity of a Charles Schwab card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Charles Schwab card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise

provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



Make the most of your
Schwab Bank Visa®
Platinum Debit Card.

[Open a Checking Account](#)



Contactless.

Pay securely and without making contact. All you have to do is tap and hold your Schwab Bank Visa Platinum Debit Card at a contactless-enabled terminal. Each transaction is accompanied by a one-time code so no personal information is exchanged. You can still insert or swipe your card if contactless isn't available. It's easy, convenient, and safe.

[Contactless FAQs >](#)



Make your phone your new wallet.

Add your Schwab Bank Visa Platinum Debit Card to your mobile wallet¹ for a more secure, convenient, and easy way to pay. At checkout, just click, glance, or touch and hold your device near the reader to pay. It's safe, secure, and simple.

[Mobile wallet FAQs >](#)



1

Open the app.

Download or locate the mobile wallet app (it is most likely already loaded on your smart device).

2

Add your card.

Add your Schwab Bank Visa Platinum Debit Card information to the mobile wallet.

3

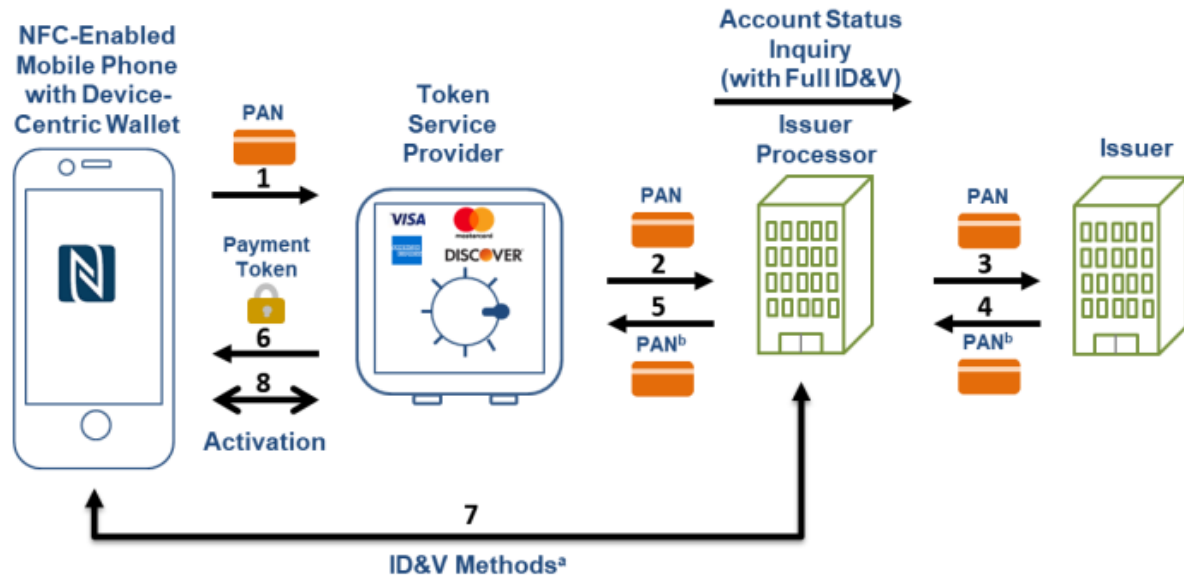
Prepare to shop.

When you check out at participating merchants, access your debit card and just click, glance, or touch and hold your device near the reader to pay. It's safe, secure and simple.

(Source: <https://www.schwab.com/checking/debit-card>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

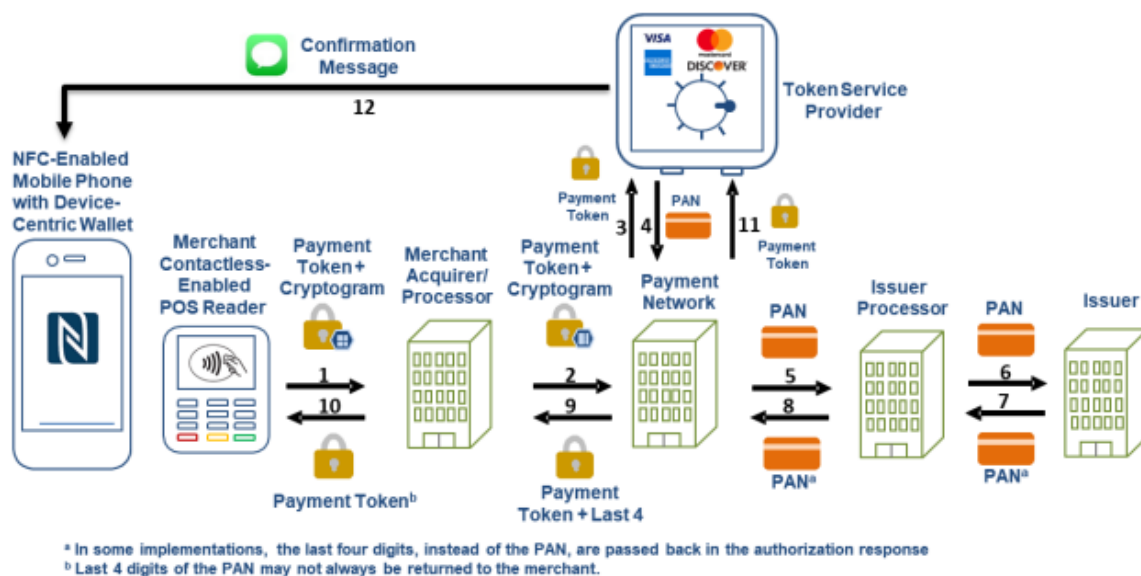


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

47. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a Charles Schwab account holder requests Charles Schwab to provision a specific Charles Schwab debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Charles Schwab card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the

request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

48. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Charles Schwab card account holders for provisioning a specific Charles Schwab debit and/or credit card for use on their mobile devices. This messaging gateway is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to receive the messages.

49. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate a key string adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the message gateway and in secure communication therewith is an authorization server that generates a token corresponding to the debit and/or credit card account number. The authorization server is either hosted directly

by Charles Schwab or through an agent with whom Charles Schwab has contracted to provide the authentication services.

50. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive transaction specific information that was input into the request by the merchant, *e.g.*, the merchant ID, invoice number, invoice amount, and date/timestamp. The interface is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to provide the authentication services.

51. The Accused Instrumentality includes a first set of instructions further operable to communicate the key string to the authorized user that the requester purports to be. For example, the messaging gateway sends the generated token to the authorized user's mobile device for use in merchant transactions.

52. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

53. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For

example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

54. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

55. Defendants thus infringe one or more claims of the 802 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 802 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 802 Patents.

56. Charles Schwab has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

57. Charles Schwab has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 802 Patent by others and Charles Schwab will continue to do so unless enjoined by this Court. Charles

Schwab's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 802 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Charles Schwab knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 802 Patent.

58. Charles Schwab continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 802 Patent.

59. Charles Schwab has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 802 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for

use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

60. Charles Schwab has committed these acts of infringement without license or authorization.

61. By engaging in the conduct described herein, Charles Schwab has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Charles Schwab is thus liable to Textile for infringement of the 802 Patent, pursuant to 35 U.S.C. § 271.

62. As a direct and proximate result of Charles Schwab's infringement of the 802 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Charles Schwab's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

63. In addition, the infringing acts and practices of Charles Schwab have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Charles Schwab is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Charles Schwab is finally and permanently enjoined from further infringement.

64. Charles Schwab has had actual knowledge of the 802 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Charles Schwab will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 802 Patent.

65. Charles Schwab has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 802 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

66. Textile has been damaged as a result of the infringing conduct by Charles Schwab alleged above. Thus, Charles Schwab is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

67. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 802 Patent.

COUNT III

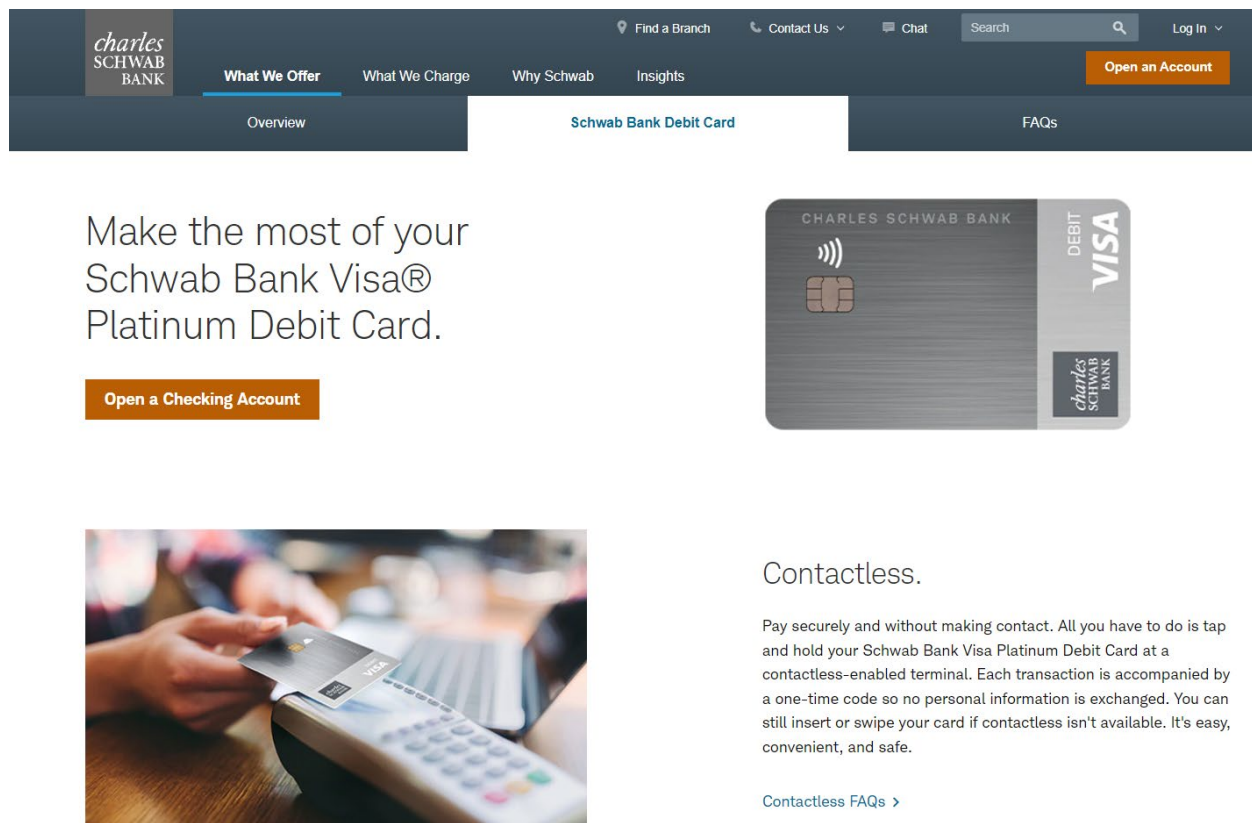
INFRINGEMENT OF U.S. PATENT NO. 9,584,499

68. On February 28, 2017, United States Patent No. 9,584,499 (“the 499 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

69. Textile is the owner of the 499 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 499 Patent against infringers, and to collect damages for all relevant times.

70. Charles Schwab offers debit and/or credit cards, such as the Schwab Bank Visa Platinum Debit Cards, that are used by Charles Schwab in practicing a method for authorizing transaction specific access to a secured resource having a secured resource identity (the “Accused Instrumentality”). The Charles Schwab transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card

number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



Make the most of your Schwab Bank Visa® Platinum Debit Card.

[Open a Checking Account](#)

CHARLES SCHWAB BANK DEBIT **VISA**

CHARLES SCHWAB BANK

Contactless.

Pay securely and without making contact. All you have to do is tap and hold your Schwab Bank Visa Platinum Debit Card at a contactless-enabled terminal. Each transaction is accompanied by a one-time code so no personal information is exchanged. You can still insert or swipe your card if contactless isn't available. It's easy, convenient, and safe.

[Contactless FAQs >](#)



Make your phone your new wallet.

Add your Schwab Bank Visa Platinum Debit Card to your mobile wallet¹ for a more secure, convenient, and easy way to pay. At checkout, just click, glance, or touch and hold your device near the reader to pay. It's safe, secure, and simple.

[Mobile wallet FAQs >](#)



1

Open the app.

Download or locate the mobile wallet app (it is most likely already loaded on your smart device).

2

Add your card.

Add your Schwab Bank Visa Platinum Debit Card information to the mobile wallet.

3

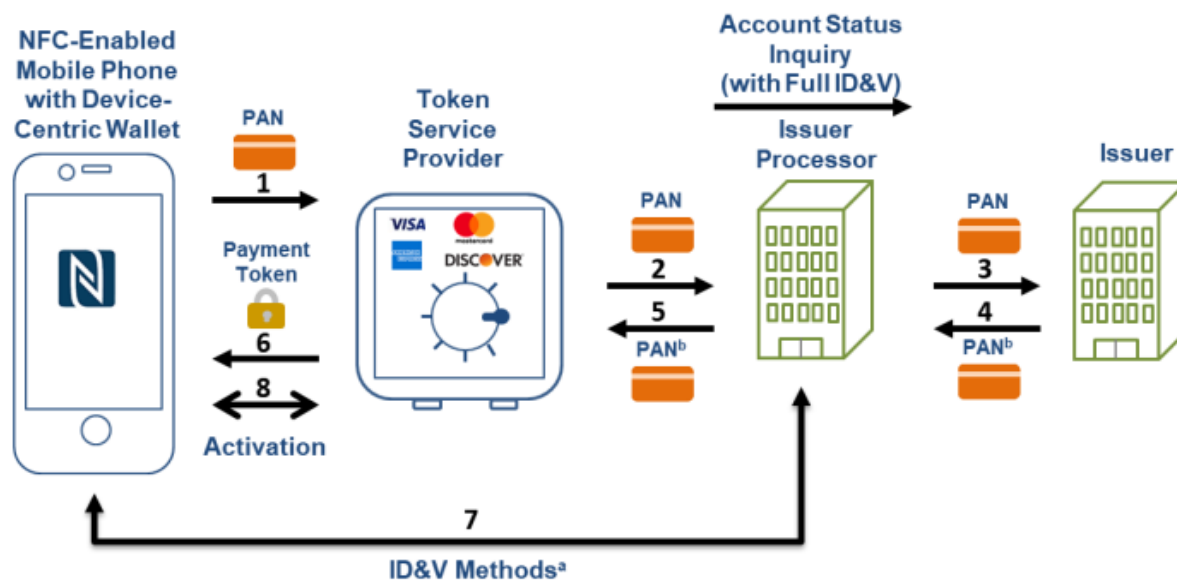
Prepare to shop.

When you check out at participating merchants, access your debit card and just click, glance, or touch and hold your device near the reader to pay. It's safe, secure and simple.

(Source: <https://www.schwab.com/checking/debit-card>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

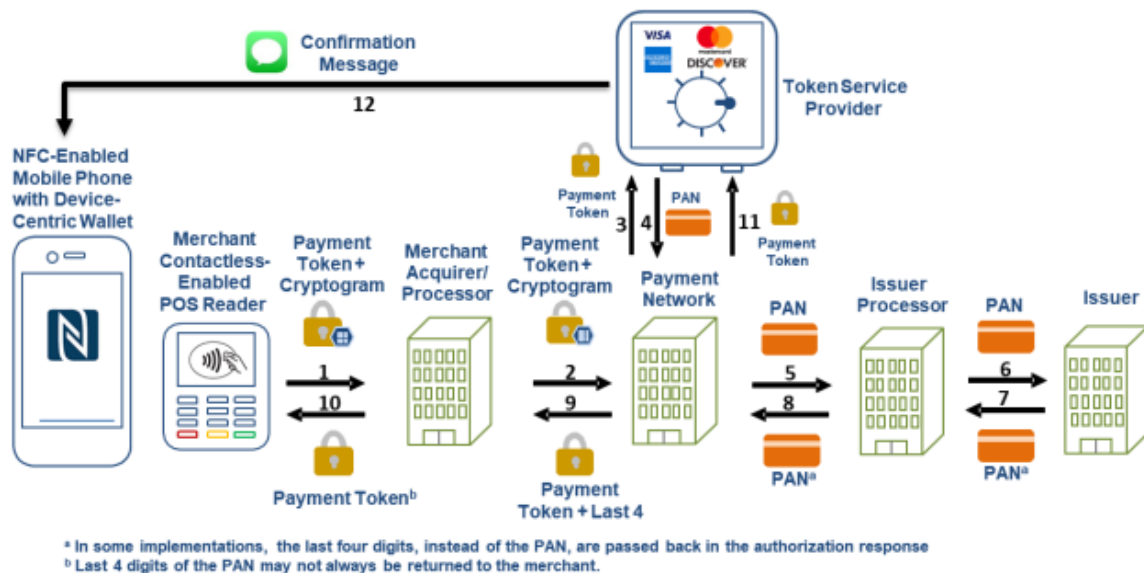


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

71. Charles Schwab's use of the Accused Instrumentality includes a method for authorizing transaction specific access to a secured resource having a secured resource identity. For example, a Charles Schwab account holder requests Charles Schwab to provision a specific Charles Schwab debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Charles Schwab card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the

request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram.

72. The Accused Instrumentality includes receiving at a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive a request for transaction specific access to a secured resource by a service client. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Charles Schwab card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Charles Schwab card account of the account holder. This messaging gateway is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to receive the messages.

73. The Accused Instrumentality includes generating a key string with a server in communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate the key string known to both said server and an authorized user of the secured resource, said key string being associated with the secured resource within a key string table accessible by the server and providing a basis for authenticating the secured resource identity by searching the key string table for the key string. For example, behind the firewall of the messaging gateway and in communication therewith is

an authorization server that generates a token corresponding to a secured resource during the provisioning process. After this, the authorization server updates a table that maps token numbers to secured resource identities. The authorization server is then able to search the table to authenticate a secured resource identity by searching the table for the token. If the token has a corresponding secured resource identity, that identity is authenticated. The authorization server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to provide the authentication services.

74. The Accused Instrumentality includes determining transaction specific information with the server in communication with the messaging gateway, the server having a third set of instructions embodied in a computer readable medium operable to identify transaction specific information within the request. For example, the authorization server is also programmed to identify within the payment authorization request transaction specific information that was passed by the merchant. The authorization server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to provide the authentication services.

75. The Accused Instrumentality includes communicating said key string to said authorized user. For example, once the provisioning process is complete, the messaging gateway and/or the server send the token to the authorized user's mobile device. The messaging gateway is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to provide the authentication services. The authorization server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to provide the authentication services.

76. The Accused Instrumentality includes receiving an authentication credential from said service client, said authentication credential having been provided to said service client by said authorized user. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant. The authorization server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to provide the authentication services.

77. The Accused Instrumentality includes evaluating said authentication credential. For example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authorizes the transaction specific access. The authorization server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to provide the authentication services.

78. The Accused Instrumentality includes wherein the key string and authentication credential do not reveal any primary identifier associated with said secured resource. For example, neither the token nor the cryptogram reveals the debit and/or credit card number associated with the secured resource.

79. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

80. Defendants thus infringe one or more claims of the 499 Patent. The elements and conduct described herein are covered by and infringe upon at least Claim 3 of the 499 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 499 Patent.

81. Charles Schwab has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

82. Charles Schwab has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 499 Patent by others and Charles Schwab will continue to do so unless enjoined by this Court. Charles Schwab's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 499 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Charles Schwab knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing,

importing, selling and/or offering to sell the Accused Instrumentality would infringe the 499 Patent.

83. Charles Schwab continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 499 Patent.

84. Charles Schwab has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 499 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

85. Charles Schwab has committed these acts of infringement without license or authorization.

86. By engaging in the conduct described herein, Charles Schwab has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Charles Schwab is thus liable to Textile for infringement of the 499 Patent, pursuant to 35 U.S.C. § 271.

87. As a direct and proximate result of Charles Schwab's infringement of the 499 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Charles Schwab's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

88. In addition, the infringing acts and practices of Charles Schwab have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Charles Schwab is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Charles Schwab is finally and permanently enjoined from further infringement.

89. Charles Schwab has had actual knowledge of the 499 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Charles Schwab will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 499 Patent.

90. Charles Schwab has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 499 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

91. Textile has been damaged as a result of the infringing conduct by Charles Schwab alleged above. Thus, Charles Schwab is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

92. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 499 Patent.

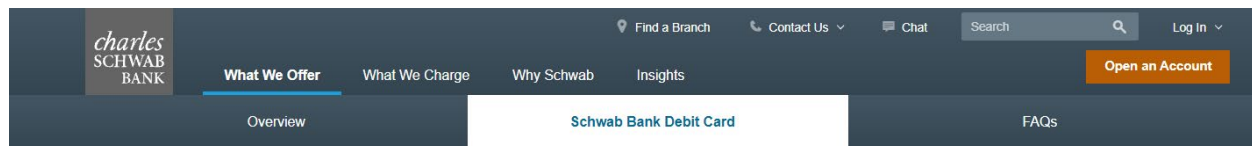
COUNT IV

INFRINGEMENT OF U.S. PATENT NO. 10,148,659

93. On December 4, 2018, United States Patent No. 10,148,659 (“the 659 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

94. Textile is the owner of the 659 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 659 Patent against infringers, and to collect damages for all relevant times.

95. Charles Schwab offers debit and/or credit cards, such as the Schwab Bank Visa Platinum Debit Cards, that are used with a computer-implemented system for a credit or debit and/or credit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit and/or credit card account number to the merchant (the “Accused Instrumentality”). The Charles Schwab transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.



Make the most of your
Schwab Bank Visa®
Platinum Debit Card.

[Open a Checking Account](#)



Contactless.

Pay securely and without making contact. All you have to do is tap and hold your Schwab Bank Visa Platinum Debit Card at a contactless-enabled terminal. Each transaction is accompanied by a one-time code so no personal information is exchanged. You can still insert or swipe your card if contactless isn't available. It's easy, convenient, and safe.

[Contactless FAQs >](#)



Make your phone your new wallet.

Add your Schwab Bank Visa Platinum Debit Card to your mobile wallet¹ for a more secure, convenient, and easy way to pay. At checkout, just click, glance, or touch and hold your device near the reader to pay. It's safe, secure, and simple.

[Mobile wallet FAQs >](#)



1

Open the app.

Download or locate the mobile wallet app (it is most likely already loaded on your smart device).

2

Add your card.

Add your Schwab Bank Visa Platinum Debit Card information to the mobile wallet.

3

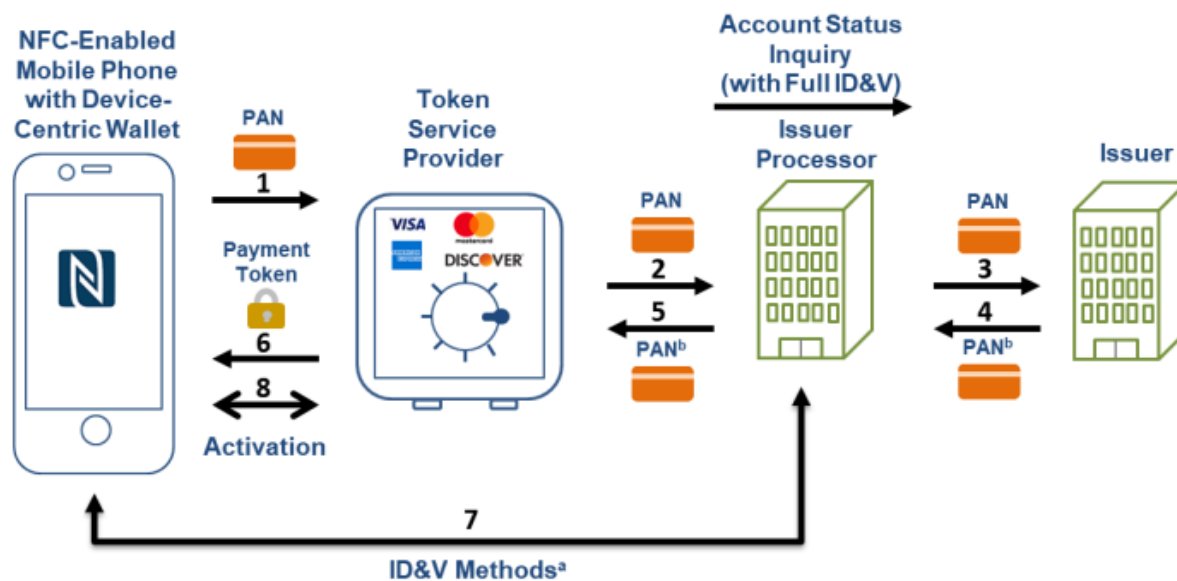
Prepare to shop.

When you check out at participating merchants, access your debit card and just click, glance, or touch and hold your device near the reader to pay. It's safe, secure and simple.

(Source: <https://www.schwab.com/checking/debit-card>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

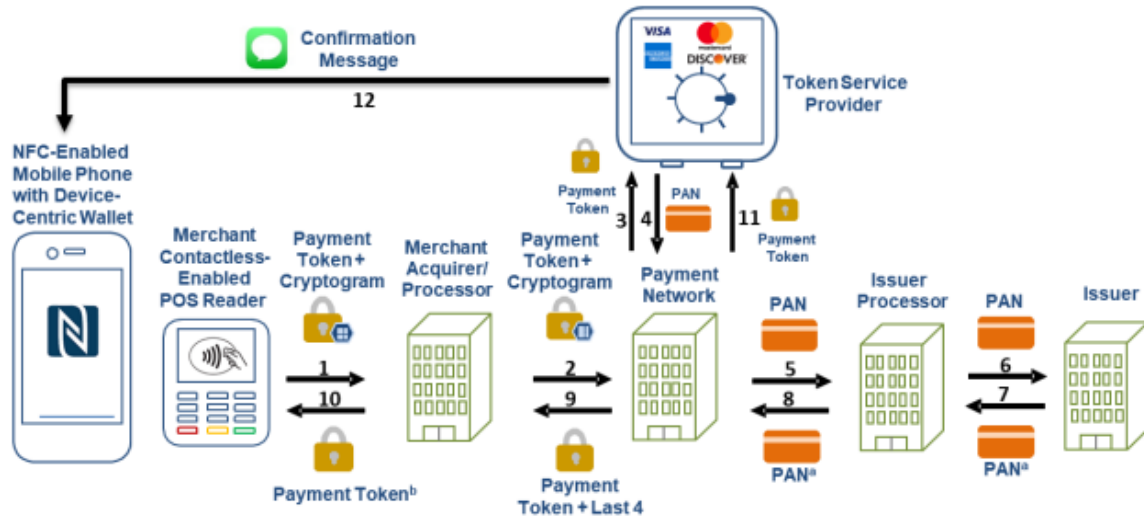
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

96. The Accused Instrumentality includes a computer-implemented system for a credit or debit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit card account number to the merchant. For example, a Charles Schwab account holder requests Charles Schwab to provision a specific Charles Schwab debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Charles Schwab to a specific merchant in a specific amount for a specific

transaction from a specific Charles Schwab card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

97. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a credit or debit card account holder's mobile device, a merchant's payment application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a Charles Schwab card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Charles Schwab card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Charles Schwab card account of the account holder. This interface is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to receive the messages.

98. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration

information received from the credit or debit card account holder through the at least one interface, the registration information comprising a credit or debit card account holder identifier and at least one credit or debit card account number having an associated unique account identifier wherein the credit or debit card account number and unique account identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card and the debit and/or credit card account number (which has a corresponding token), received from Charles Schwab card account holders through the interface for provisioning a specific Charles Schwab debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Charles Schwab card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Charles Schwab card account of the account holder. The server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to receive the messages.

99. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to pay the specific merchant for the specific transaction from a given debit or credit card account, the authorization request message having been received through the at least one interface and originating from the credit or debit card account holder's mobile device and comprising: a first merchant identifier; a first transaction specific information selected from the group consisting of a first transaction amount and first client reference identifier; the credit or debit card account holder identifier; and a designated unique account identifier selected from the at least one unique account identifiers. For example, the Accused

Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Charles Schwab card account holder's mobile device. The server is programmed to receive authorization requests initiated by Charles Schwab card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a merchant identifier, and the Charles Schwab card account holder identifier. The server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to receive the messages.

100. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string wherein the key string is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the designated unique account identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to receive the messages.

101. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive a payment request message from the merchant's payment application through the at least one interface, the payment request message comprising: a second merchant identifier; a second transaction specific information selected from the group consisting of a second transaction amount and second client reference identifier; and a second transaction specific authentication credential whereby the second authentication credential was received by the merchant application from the credit or debit card account holder's mobile device. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Charles Schwab card account holder's mobile device. The server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to receive the messages.

102. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the credit or debit card account holder's request to use the credit or debit card account number associated with the designated unique account identifier for payment to the specific merchant for the specific transaction and authorizing the resource provider to use the credit or debit card account number associated with the designated unique account identifier to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or bank account number to the

specific merchant by determining if: the first merchant identifier matches the second merchant identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to provide the authentication services.

103. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

104. Defendants thus infringe one or more claims of the 659 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 9 of the 659 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 659 Patent.

105. Charles Schwab has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

106. Charles Schwab has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 659 Patent by others and Charles Schwab will continue to do so unless enjoined by this Court. Charles Schwab's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 659 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Charles Schwab knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 659 Patent.

107. Charles Schwab continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as

consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 659 Patent.

108. Charles Schwab has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 659 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

109. Charles Schwab has committed these acts of infringement without license or authorization.

110. By engaging in the conduct described herein, Charles Schwab has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Charles Schwab is thus liable to Textile for infringement of the 659 Patent, pursuant to 35 U.S.C. § 271.

111. As a direct and proximate result of Charles Schwab's infringement of the 659 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Charles Schwab's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

112. In addition, the infringing acts and practices of Charles Schwab have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Charles Schwab is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Charles Schwab is finally and permanently enjoined from further infringement.

113. Charles Schwab has had actual knowledge of the 659 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Charles Schwab will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 659 Patent.

114. Charles Schwab has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 659 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

115. Textile has been damaged as a result of the infringing conduct by Charles Schwab alleged above. Thus, Charles Schwab is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

116. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 659 Patent.

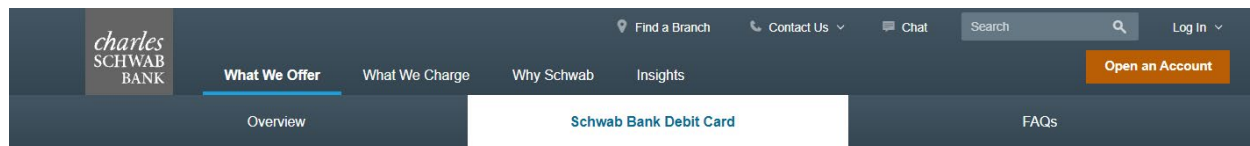
COUNT V

INFRINGEMENT OF U.S. PATENT NO. 10,560,454

117. On February 11, 2020, United States Patent No. 10,560,454 (“the 454 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

118. Textile is the owner of the 454 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 454 Patent against infringers, and to collect damages for all relevant times.

119. Charles Schwab offers debit and/or credit cards, such as the Schwab Bank Visa Platinum Debit Cards, that are used with a computer-implemented system for a user to authorize a resource authorize a service client’s access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource’s common identifier to the service client (the “Accused Instrumentality”). The Charles Schwab transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.



Make the most of your
Schwab Bank Visa®
Platinum Debit Card.

[Open a Checking Account](#)



Contactless.

Pay securely and without making contact. All you have to do is tap and hold your Schwab Bank Visa Platinum Debit Card at a contactless-enabled terminal. Each transaction is accompanied by a one-time code so no personal information is exchanged. You can still insert or swipe your card if contactless isn't available. It's easy, convenient, and safe.

[Contactless FAQs >](#)



Make your phone your new wallet.

Add your Schwab Bank Visa Platinum Debit Card to your mobile wallet¹ for a more secure, convenient, and easy way to pay. At checkout, just click, glance, or touch and hold your device near the reader to pay. It's safe, secure, and simple.

[Mobile wallet FAQs >](#)



1

Open the app.

Download or locate the mobile wallet app (it is most likely already loaded on your smart device).

2

Add your card.

Add your Schwab Bank Visa Platinum Debit Card information to the mobile wallet.

3

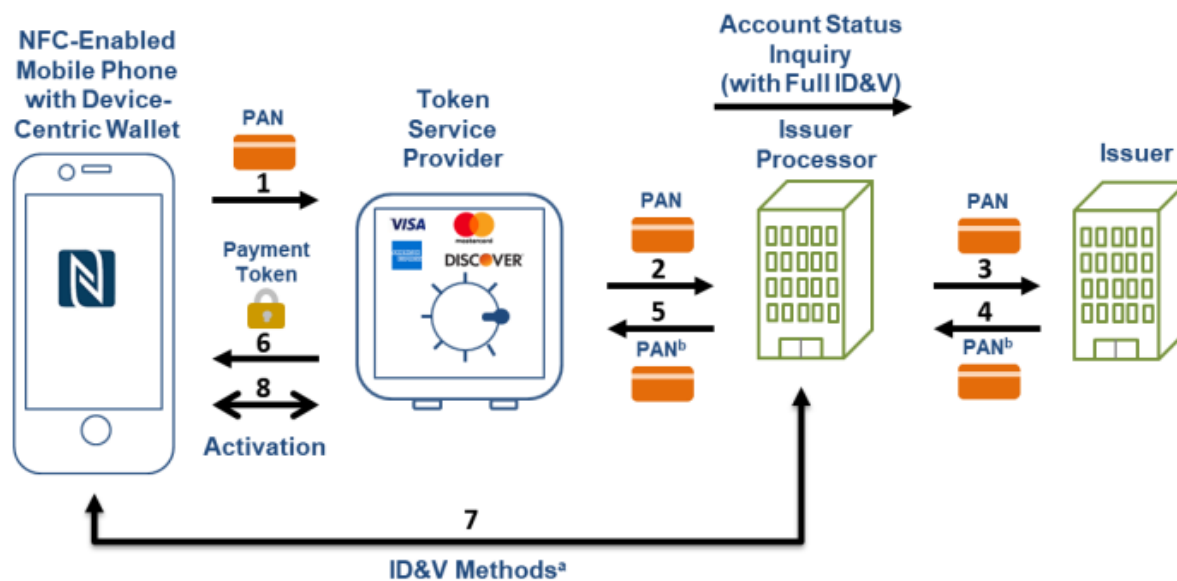
Prepare to shop.

When you check out at participating merchants, access your debit card and just click, glance, or touch and hold your device near the reader to pay. It's safe, secure and simple.

(Source: <https://www.schwab.com/checking/debit-card>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

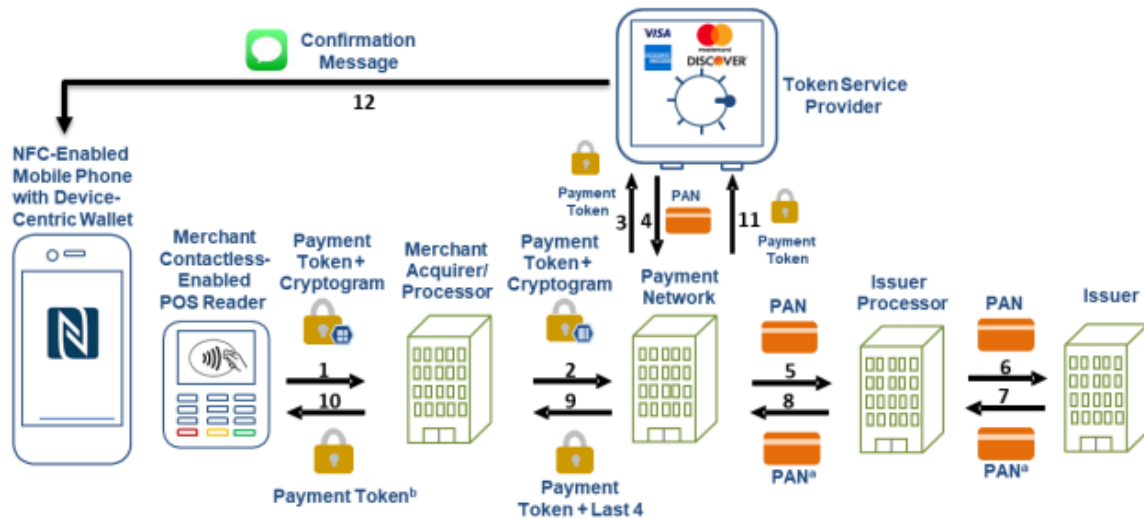
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

120. The Accused Instrumentality includes a computer-implemented system for a user to authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client. For example, a Charles Schwab account holder requests Charles Schwab to provision a specific Charles Schwab debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Charles Schwab to a specific merchant in a specific amount for a specific transaction from a specific Charles Schwab card

account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

121. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a user's application, a service client's application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a Charles Schwab card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Charles Schwab card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Charles Schwab card account of the account holder. This interface is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to receive the messages.

122. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration

information received from the user through the at least one interface, the registration information comprising a user identifier and at least one secured resource identifier associated with the common identifier of the secured resource, wherein the common identifier and secured resource identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card, the debit and/or credit card account number (which has a corresponding token), and the CVV number received from Charles Schwab card account holders through the interface for provisioning a specific Charles Schwab debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Charles Schwab card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Charles Schwab card account of the account holder. The server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to receive the messages.

123. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to authorize access to the secured resource by the service client, the authorization request message having been received through the at least one interface from the user's application and comprising: a first service client identifier; a first transaction specific information; the user identifier; and a designated secured resource identifier selected from one of the at least one secured resource identifiers. For example, the Accused Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Charles Schwab

card account holder's mobile device. The server is programmed to receive authorization requests initiated by Charles Schwab card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a CVV number, a merchant identifier, other token information, and the Charles Schwab card account holder identifier. The server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to receive the messages.

124. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string and does not include or reveal the common identifier associated with the designated secured resource identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to receive the messages.

125. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive an access request message from the service client's application through the at least one interface, the

payment request message comprising: a second service client identifier; a second transaction specific information; and a second transaction specific authentication credential whereby the second transaction specific authentication credential was received by the service client's application from the user's application. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Charles Schwab card account holder's mobile device. The server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to receive the messages.

126. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the user's request to access the secured resource associated with the designated secured resource identifier without transmitting or otherwise providing the common identifier of the secured resource to the service client by determining if: the first service client identifier matches the second service client identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of

requestor as the actual account holder. The server is either hosted directly by Charles Schwab or through an agent with whom Charles Schwab has contracted to provide the authentication services.

127. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

128. Defendants thus infringe one or more claims of the 454 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 8 of the 454 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 454 Patent.

129. Charles Schwab has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

130. Charles Schwab has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 454 Patent by others and Charles Schwab will continue to do so unless enjoined by this Court. Charles

Schwab's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 454 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Charles Schwab knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 454 Patent.

131. Charles Schwab continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 454 Patent.

132. Charles Schwab has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 454 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an

infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

133. Charles Schwab has committed these acts of infringement without license or authorization.

134. By engaging in the conduct described herein, Charles Schwab has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Charles Schwab is thus liable to Textile for infringement of the 454 Patent, pursuant to 35 U.S.C. § 271.

135. As a direct and proximate result of Charles Schwab's infringement of the 454 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Charles Schwab's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

136. In addition, the infringing acts and practices of Charles Schwab have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Charles Schwab is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Charles Schwab is finally and permanently enjoined from further infringement.

137. Charles Schwab has had actual knowledge of the 454 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Charles Schwab will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 454 Patent.

138. Charles Schwab has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 454 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

139. Textile has been damaged as a result of the infringing conduct by Charles Schwab alleged above. Thus, Charles Schwab is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

140. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 454 Patent.

ADDITIONAL ALLEGATIONS REGARDING INFRINGEMENT

141. Charles Schwab has also indirectly infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by inducing others to directly infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Charles Schwab has induced the end-users, Charles Schwab’s customers, to directly infringe (literally and/or under the doctrine of equivalents) the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by using the Accused Instrumentality.

142. Charles Schwab took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

143. Such steps by Charles Schwab included, among other things, advising or directing customers and end-users to use the Accused Instrumentality in an infringing manner; advertising

and promoting the use of the Accused Instrumentality in an infringing manner; and/or distributing instructions that guide users to use the Accused Instrumentality in an infringing manner.

144. Charles Schwab has performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts constitute infringement, at least since the filing of the Complaint.

145. Charles Schwab was and is aware that the normal and customary use of the Accused Instrumentality by Charles Schwab's customers would infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Charles Schwab's inducement is ongoing.

146. Charles Schwab directs or controls the use of the Accused Instrumentality nationwide through its own websites and in its own branches, including in Texas and elsewhere in the United States, and expects and intends that the Accused Instrumentality will be so used.

147. Charles Schwab took active steps, directly and/or through contractual relationships with others, with the specific intent to cause such persons to make or use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

148. Charles Schwab performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts would constitute infringement.

149. Charles Schwab's inducement is ongoing.

150. Charles Schwab has also indirectly infringed by contributing to the infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Charles Schwab has contributed to the direct infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by the end-user of the Accused Instrumentality.

151. The Accused Instrumentality has special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

152. As described above, the special features include securely authorizing specific transactions without providing a credit or debit card number to the merchant used in a manner that infringes the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

153. The special features constitute a material part of the invention of one or more of the claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and are not staple articles of commerce suitable for substantial non-infringing use.

154. Charles Schwab's contributory infringement is ongoing.

155. Charles Schwab's actions are at least objectively reckless as to the risk of infringing valid patents and this objective risk was either known or should have been known by Charles Schwab, at least since the filing of the Complaint.

156. Charles Schwab has had knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent at least since the filing of the Complaint.

157. Charles Schwab's customers have infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

158. Charles Schwab encouraged its customers' infringement.

159. Charles Schwab's direct and indirect infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent is, has been, and/or continues to be willful, intentional, deliberate, and/or in conscious disregard of Textile's rights under the patents.

160. Textile has been damaged as a result of the infringing conduct by Charles Schwab alleged above. Thus, Charles Schwab is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Textile hereby requests a trial by jury on all issues so triable by right.

PRAYER FOR RELIEF

Textile requests that the Court find in its favor and against Charles Schwab, and that the Court grant Textile the following relief:

- a. Judgment that one or more claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent have been infringed, either literally and/or under the doctrine of equivalents, by Charles Schwab and/or all others acting in concert therewith;
- b. A permanent injunction enjoining Charles Schwab and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert therewith from infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent; or, in the alternative, an award of a reasonable ongoing royalty for future infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by such entities;
- c. Judgment that Charles Schwab account for and pay to Textile all damages to and

costs incurred by Textile because of Charles Schwab's infringing activities and other conduct complained of herein, including an award of all increased damages to which Textile is entitled under 35 U.S.C. § 284;

d. That Textile be granted pre-judgment and post-judgment interest on the damages caused by Charles Schwab's infringing activities and other conduct complained of herein;

e. That this Court declare this an exceptional case and award Textile its reasonable attorney's fees and costs in accordance with 35 U.S.C. § 285; and

f. That Textile be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: October 12, 2021

Respectfully submitted,

/s/ Matthew J. Antonelli

Matthew J. Antonelli

Texas Bar No. 24068432

matt@ahtlawfirm.com

Zachariah S. Harrington

Texas Bar No. 24057886

zac@ahtlawfirm.com

Larry D. Thompson, Jr.

Texas Bar No. 24051428

larry@ahtlawfirm.com

Christopher Ryan Pinckney

Texas Bar No. 24067819

ryan@ahtlawfirm.com

ANTONELLI, HARRINGTON

& THOMPSON LLP

4306 Yoakum Blvd., Ste. 450

Houston, TX 77006

(713) 581-3000

Stafford Davis

State Bar No. 24054605

sdavis@stafforddavisfirm.com

Catherine Bartles

Texas Bar No. 24104849

cbartles@stafforddavisfirm.com

THE STAFFORD DAVIS FIRM

815 South Broadway Avenue
Tyler, Texas 75701
(903) 593-7000
(903) 705-7369 fax

Of Counsel:

Sandeep Seth
Texas State Bar No. 18043000
SETHLAW
Pennzoil Place
700 Milam Street, Suite 1300
Houston, Texas 77002
Telephone: (713) 244-5017
ss@sethlaw.com

Attorneys for Textile Computer Systems, Inc.

EXHIBIT 2C

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

TEXTILE COMPUTER SYSTEMS, INC.,

Plaintiff,

v.

COMERICA BANK,

Defendant.

CIVIL ACTION NO. 6:21-cv-1052

ORIGINAL COMPLAINT FOR
PATENT INFRINGEMENT

JURY TRIAL DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Textile Computer Systems, Inc. (“Textile” or “Plaintiff”) files this original complaint against Defendant Comerica Bank (“Comerica”), alleging, based on its own knowledge as to itself and its own actions and based on information and belief as to all other matters, as follows:

PARTIES

1. Textile Computer Systems, Inc. is a corporation formed under the laws of the State of Texas, with a place of business at 618 Bluff Trail, San Antonio, Texas, 78216.
2. Comerica Bank is a company duly organized and existing under the laws of Texas. Comerica Bank has places of business in Austin, Texas and San Antonio, Texas.
3. Comerica and its affiliates lead and are part of an interrelated group of companies which together comprise one of the country’s largest banking and financial service entities, including under the Comerica brand.
4. Comerica and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

5. Comerica and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

6. Comerica and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

7. Thus, Comerica and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

JURISDICTION AND VENUE

8. This is an action for infringement of United States patents arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. § 1331 and § 1338(a).

9. This Court has personal jurisdiction over Comerica pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Comerica has done and continues to do business in Texas; and (ii) Comerica has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations, inducing others to commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein.

10. Venue is proper in this district pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Comerica has committed and continues to commit acts of patent infringement in this district. For example, Comerica cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those

cardholders make and/or use the accused instrumentalities in the district. Comerica induces others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. Comerica has regular and established places of business in this district, including at least at 13750 San Pedro, Suite 100, San Antonio, Texas 78232, at 100 N Santa Rosa St., Suite 110, San Antonio, Texas 78207, and at numerous other locations in San Antonio and Austin:

Comerica Personal Small Business Commercial Wealth Management

Find a Comerica location near you.

san antonio Find Use Current Location

Highway 281

Map Satellite

Address
13750 San Pedro
Suite 100
San Antonio, TX 78232
Phone (210) 491-3600
Fax (210) 277-3141

Manager
Crystal Alaniz
Work (210) 491-3600

Banking Center

Mon.	9:00 AM - 4:00 PM
Tues.	9:00 AM - 4:00 PM
Wed.	9:00 AM - 4:00 PM
Thurs.	9:00 AM - 4:00 PM
Fri.	9:00 AM - 5:00 PM

[Schedule Appointment](#)

[Driving Directions](#)

(Source: <https://locations.comerica.com/location/highway-281?q=san+antonio>)



(Source: screenshot from Google Maps Street View)

Comerica® Personal Small Business Commercial Wealth Management

Find a Comerica location near you.

san antonio Find Use Current Location

Downtown San Antonio

Address
100 N Santa Rosa St
Suite 110
San Antonio, TX 78207
Phone (210) 222-2216

Manager
Luis Zuniga
Work (210) 222-2216

[Schedule Appointment](#)

[Driving Directions](#)

Banking Center

Mon.	9:00 AM - 4:00 PM
Tues.	9:00 AM - 4:00 PM
Wed.	9:00 AM - 4:00 PM
Thurs.	9:00 AM - 4:00 PM
Fri.	9:00 AM - 5:00 PM

Drive Through

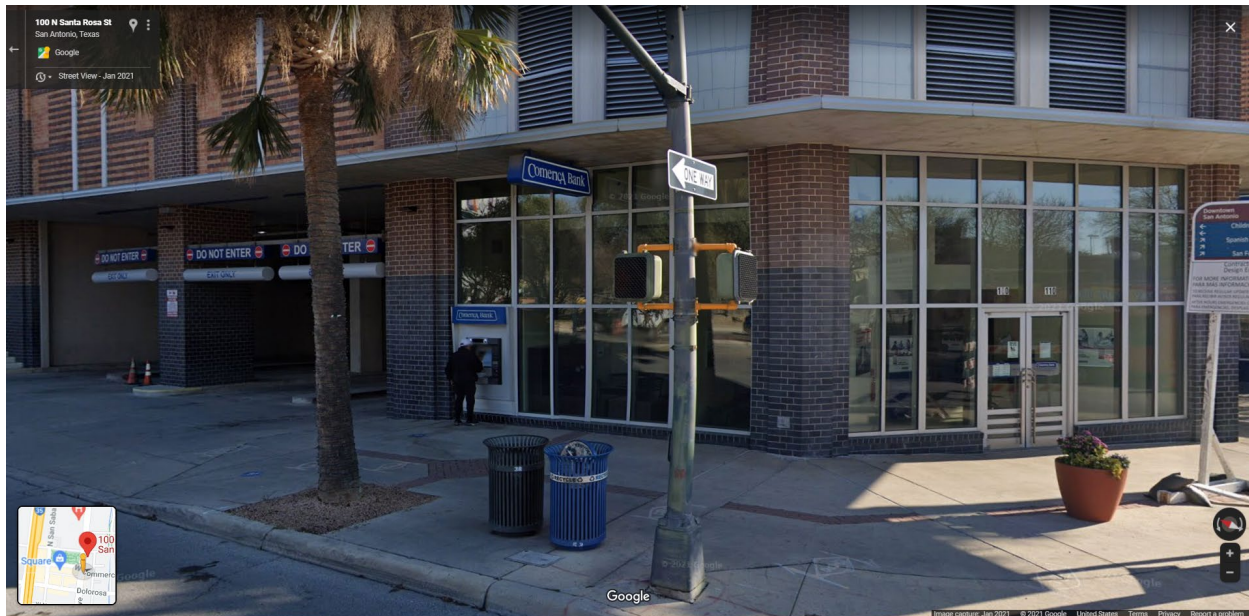
Mon.	8:00 AM - 5:00 PM
Tues.	8:00 AM - 5:00 PM
Wed.	8:00 AM - 5:00 PM
Thurs.	8:00 AM - 5:00 PM
Fri.	8:00 AM - 5:00 PM

ATM

Functionality
Full Service, Envelope-Free Deposits

Availability
24 hours a day 7 days a week

(Source: <https://locations.comerica.com/location/downtown-san-antonio?q=san+antonio>)



(Source: screenshot from Google Maps Street View)

BACKGROUND

11. The patents-in-suit generally pertain to payment authorization technology used in payment networks used to process transactions from, for example, credit cards and debit cards. The technology disclosed by the patents was developed by Gopal Nandakumar, a Texas-based entrepreneur, software engineer, and prolific inventor with over 30 years of experience in the field of Information Management Systems.

12. In 1987, after receiving Master's Degrees from both the University of Madras, India and the Georgia Institute of Technology, Mr. Nandakumar formed Textile Computer Systems, Inc. ("Textile") for the purpose of consulting and developing software for the textile industry. In 2005, Textile began transitioning into credit card transaction systems. In 2011, Textile began to develop and market the MySingleLink suite of applications.

13. The Nandakumar patents are related to payment authorization technology. Mr. Nandakumar has been at the forefront of payment authorization, developing, disclosing, and patenting solutions for reducing fraud in credit and debit card transactions. Indeed, the

Nandakumar patents (or the applications leading to them) have been cited during patent prosecution over a hundred times, including by numerous leading companies in the payment authorization industry such as ADP, Bank of America, Google, Groupon, IBM, Mastercard, NEC, Paypal, Visa, and Wells Fargo.

THE TECHNOLOGY

14. The patents-in-suit, U.S. Patent Nos. 8,505,079, 8,533,802, 9,584,499, 10,148,659, and 10,560,454 (collectively, the “Asserted Patents”), teach systems, including payment processing systems, for securely and effectively approving and processing specific credit card and/or debit card transactions. Through the specific use of servers, messaging gateways, and/or interfaces, these systems act to reduce credit card and/or debit card fraud and misuse through their use and validation of key strings, authentication credentials, transaction specific information, and transaction specific credentials. The technology in the Asserted Patents improves the underlying functionality of existing card processing infrastructure by minimizing fraud and data theft in the face of attacks on payment systems that continue to grow in their number and sophistication.

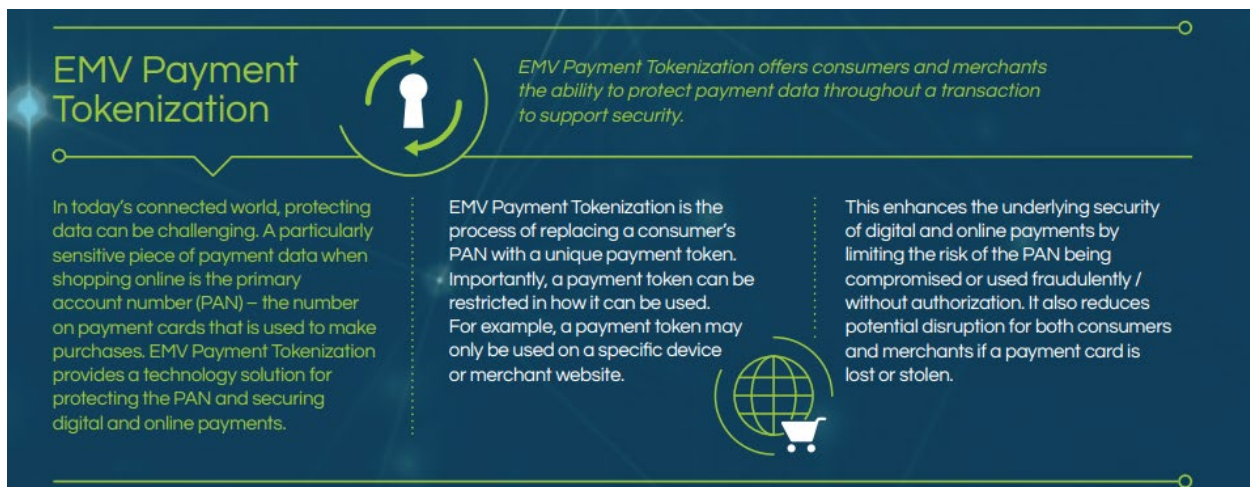
15. The patented improvements are critical for implementing secure payment systems, especially in light of the many high-profile merchant data breaches that have led to increased credit and debit card fraud. For example, in 2006, TJX Companies, who owns retailers like TJMaxx and Marshall’s, was hit with a cyber attack that resulted in the theft of credit cards leading to over \$100 million in fraud losses. In 2013, five people were indicted for attacking a number of retailers and financial institutions including NASDAQ, 7-Eleven, JCP, and others, stealing over 160 million cards. Also in 2013, the retailer Target suffered a data breach that resulted in 40 million debit and credit cards being compromised.

16. One implementation of the technology claimed in the Asserted Patents has been described by EMVCo as “a global Payment Tokenisation ecosystem that overlays and interoperates with existing payment ecosystems to support digital commerce and new methods of payment” and as “enhanc[ing] the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorized or fraudulent use of PANs.”

(Source: <https://www.emvco.com/emv-technologies/payment-tokenisation/>).

17. The technology claimed in the Asserted Patents is far from conventional technology. The payment industry gathered and consulted experts who worked together over a number of years to develop infringing payment tokenisation systems. In other words, the technology claimed in the Asserted Patents was not existing or conventional technology that the payment industry had sitting on the shelf.

18. Indeed, as recently as February of this year, EMVCo itself recognized that an implementation of the technology claimed in the Asserted Patents “provides a technology solution for protecting the PAN and securing digital and online payments”:



(Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

19. That same EMVCo document notes that “In today’s connected world, protecting data can be challenging. A particularly sensitive piece of payment data when shopping online is the primary account number (PAN) – the number on payment cards that is used to make purchases” and that EMVCo’s payment tokenization “enhances the underlying security of digital and online payments by limiting the risk of the PAN being compromised or used fraudulently / without authorization.” The document also states that the “Payment Tokenisation Specification provides an interoperable Technical Framework.” (Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

20. One of the asserted patents, the 079 Patent, was challenged in an Inter Partes Review proceeding before the Patent and Trademark Office (“PTO”). The PTO found that the challenger, Unified Patents Inc., was unable to show that one element, the “key string” as claimed in the 079 Patent claims and as construed by the PTO, was in the prior art at all, much less it being conventional or widespread. The PTO thus confirmed the patentability of all challenged claims of the 079 Patent.

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 8,505,079

21. On August 6, 2013, United States Patent No. 8,505,079 (“the 079 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

22. Textile is the owner of the 079 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 079 Patent against infringers, and to collect damages for all relevant times.

23. Comerica offers debit and/or credit cards, such as the Comerica Debit Mastercard, that are used with an authentication system that authenticates the identity of a Comerica card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Comerica card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities, for example. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.

Comerica

Personal Small Business Commercial Wealth Management

Banking Borrowing Investing Insurance

Home > Personal > Banking > Online Services > Mobile Wallet

Mobile Wallets

Your mobile device, your mobile wallet

Pay with your Comerica debit or credit card using your preferred mobile wallet.

Use your Comerica debit and credit card on Apple Pay®, Samsung Pay and Google Pay™ to make checkouts at your favorite retailers convenient, fast, and secure. Pay confidently from your mobile device knowing that the same fraud protection Comerica gives your credit and debit card carries over to your mobile wallet.

With a simple tap, click or touch, you can shop with ease in-store, online, and in-app.

In-store purchases:

Stop fumbling for your wallet. Pay with your mobile device wherever you see the contactless payment symbol at checkout.

Online and in-app purchases:

Rather than entering your credit or debit card number and address details, select your mobile wallet where accepted when shopping online and in-app to save time.

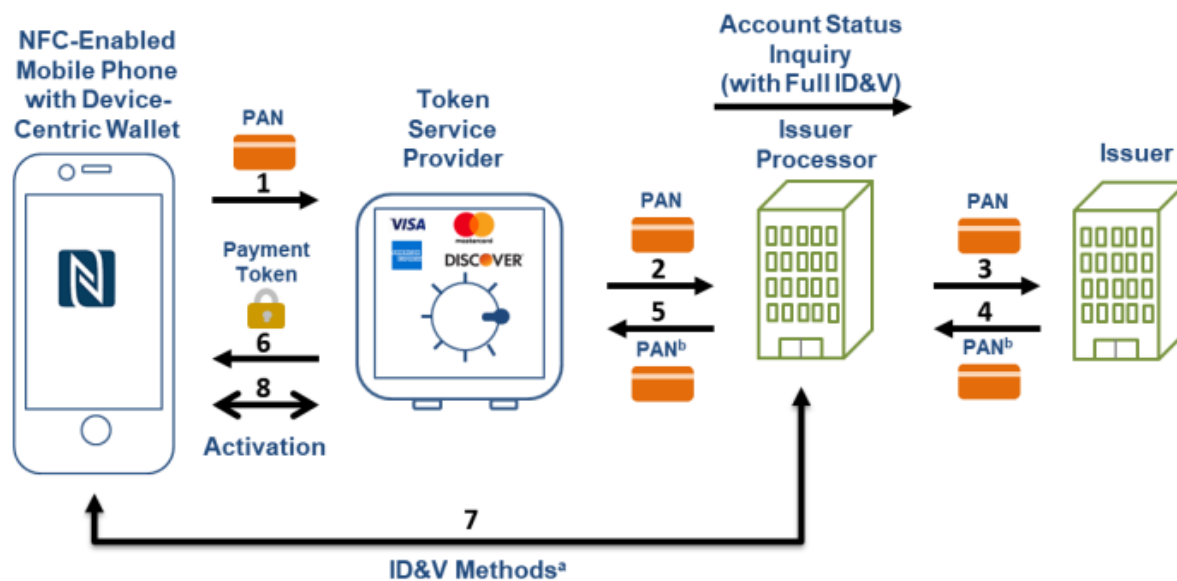
Select your mobile wallet below to learn how to add your Comerica credit or debit card, and change the way you pay today!

Click a logo below to learn more.

(Source: <https://www.comerica.com/personal-finance/banking/online-services/mobile-wallet.html>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

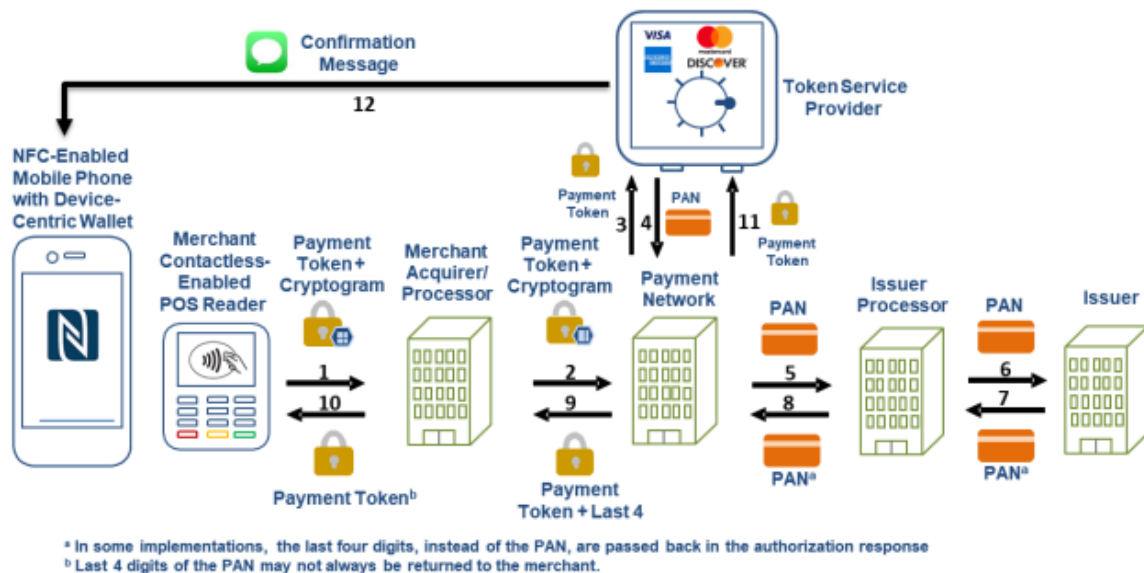


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

24. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a Comerica account holder requests Comerica to provision a specific Comerica debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Comerica card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's

smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

25. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Comerica card account holders for provisioning a specific Comerica debit and/or credit card for use on their mobile devices. The messaging gateway is also programmed to receive requests initiated by Comerica card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Comerica card account of the account holder. This messaging gateway is either hosted directly by Comerica or through an agent with whom Comerica has contracted to receive the messages.

26. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to determine a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the messaging

gateway and in secure communication therewith is an authorization server that processes the received request to identify the token value sent for the account selected to be charged that was passed from the authorized user to the merchant terminal via the NFC communication link. From the token value, the server can look up the debit and/or credit card account number. The authorization server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to provide the authentication services.

27. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive within the payment authorization request transaction specific information that was input into the request by the merchant. The interface is either hosted directly by Comerica or through an agent with whom Comerica has contracted to provide the authentication services.

28. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

29. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

30. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

31. Defendants thus infringe one or more of the claims of the 079 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 079 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 079 Patent.

32. Comerica has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(a), by making, using, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

33. Comerica has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 079 Patent by others and Comerica will continue to do so unless enjoined by this Court. Comerica's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors,

agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 079 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Comerica knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 079 Patent.

34. Comerica continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 079 Patent.

35. Comerica has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 079 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

36. Comerica has committed these acts of infringement without license or authorization.

37. By engaging in the conduct described herein, Comerica has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Comerica is thus liable to Textile for infringement of the 079 Patent, pursuant to 35 U.S.C. § 271.

38. As a direct and proximate result of Comerica's infringement of the 079 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Comerica's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

39. In addition, the infringing acts and practices of Comerica have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Comerica is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Comerica is finally and permanently enjoined from further infringement.

40. Comerica has had actual knowledge of the 079 Patent at least as of October 18, 2013, when Textile sent a letter to Ralph W. Babb, Jr., then Chief Executive Officer of Comerica Bank, that described certain implementations of the patented technology and specifically identified the 079 Patent.

41. Comerica has had actual knowledge of the 079 Patent at least as of November 10, 2014, when Textile sent a letter to Ralph W. Babb, Jr., then Chief Executive Officer of Comerica

Bank, that described certain implementations of the patented technology and specifically identified the 079 Patent.

42. Comerica has had actual knowledge of the 079 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Comerica will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 079 Patent.

43. Comerica has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 079 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

44. Textile has been damaged as a result of the infringing conduct by Comerica alleged above. Thus, Comerica is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

45. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 079 Patent.

COUNT II

INFRINGEMENT OF U.S. PATENT NO. 8,533,802

46. On September 10, 2013, United States Patent No. 8,533,802 (“the 802 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

47. Textile is the owner of the 802 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 802 Patent against infringers, and to collect damages for all relevant times.

48. Comerica offers debit and/or credit cards, such as the Comerica Debit Mastercard, that are used with an authentication system that authenticates the identity of a Comerica card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Comerica card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.

Comerica

Personal Small Business Commercial Wealth Management

Banking Borrowing Investing Insurance

Home > Personal > Banking > Online Services > Mobile Wallet

Mobile Wallets

Your mobile device, your mobile wallet

Pay with your Comerica debit or credit card using your preferred mobile wallet.

Use your Comerica debit and credit card on Apple Pay®, Samsung Pay and Google Pay™ to make checkouts at your favorite retailers convenient, fast, and secure. Pay confidently from your mobile device knowing that the same fraud protection Comerica gives your credit and debit card carries over to your mobile wallet.

With a simple tap, click or touch, you can shop with ease in-store, online, and in-app.

In-store purchases:

Stop fumbling for your wallet. Pay with your mobile device wherever you see the contactless payment symbol at checkout.

Online and in-app purchases:

Rather than entering your credit or debit card number and address details, select your mobile wallet where accepted when shopping online and in-app to save time.

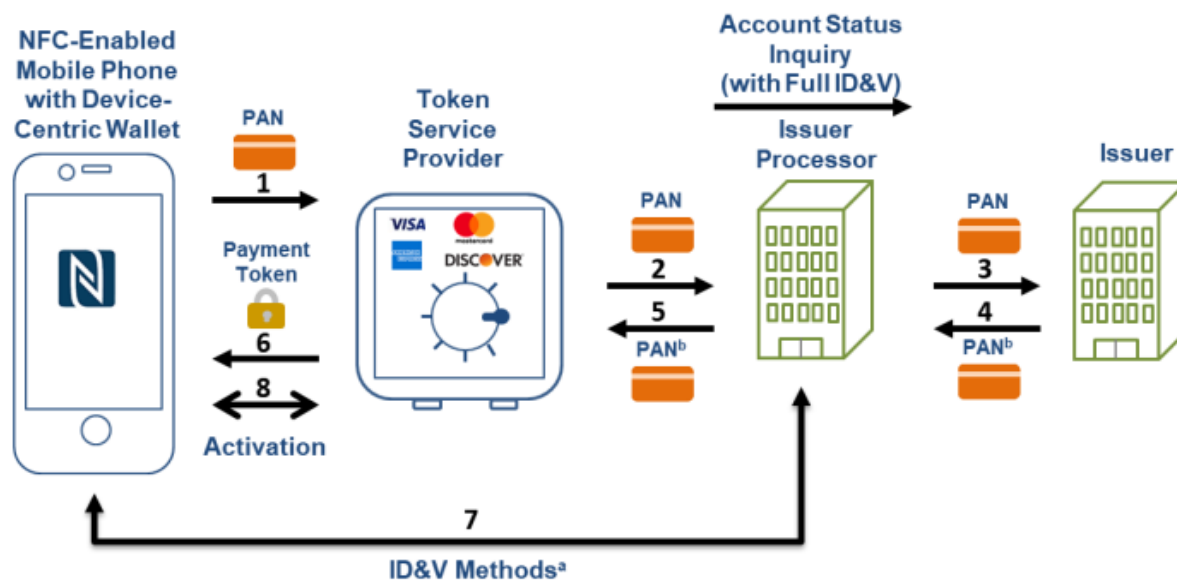
Select your mobile wallet below to learn how to add your Comerica credit or debit card, and change the way you pay today!

Click a logo below to learn more.

(Source: <https://www.comerica.com/personal-finance/banking/online-services/mobile-wallet.html>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

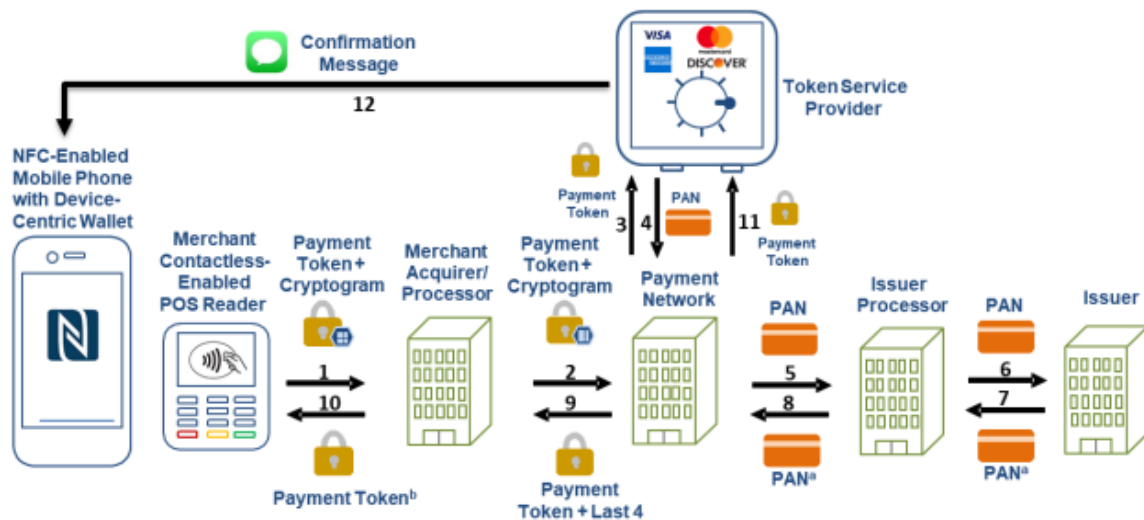
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response
^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

49. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a Comerica account holder requests Comerica to provision a specific Comerica debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Comerica card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's

smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

50. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Comerica card account holders for provisioning a specific Comerica debit and/or credit card for use on their mobile devices. This messaging gateway is either hosted directly by Comerica or through an agent with whom Comerica has contracted to receive the messages.

51. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate a key string adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the message gateway and in secure communication therewith is an authorization server that generates a token corresponding to the debit and/or credit card account number. The authorization server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to provide the authentication services.

52. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive transaction specific information that was input into the request by the merchant, *e.g.*, the merchant ID, invoice number, invoice amount, and date/timestamp. The interface is either hosted directly by Comerica or through an agent with whom Comerica has contracted to provide the authentication services.

53. The Accused Instrumentality includes a first set of instructions further operable to communicate the key string to the authorized user that the requester purports to be. For example, the messaging gateway sends the generated token to the authorized user's mobile device for use in merchant transactions.

54. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

55. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

56. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

57. Defendants thus infringe one or more claims of the 802 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 802 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 802 Patents.

58. Comerica has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

59. Comerica has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 802 Patent by others and Comerica will continue to do so unless enjoined by this Court. Comerica's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to,

encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 802 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Comerica knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 802 Patent.

60. Comerica continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 802 Patent.

61. Comerica has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 802 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

62. Comerica has committed these acts of infringement without license or authorization.

63. By engaging in the conduct described herein, Comerica has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Comerica is thus liable to Textile for infringement of the 802 Patent, pursuant to 35 U.S.C. § 271.

64. As a direct and proximate result of Comerica's infringement of the 802 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Comerica's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

65. In addition, the infringing acts and practices of Comerica have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Comerica is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Comerica is finally and permanently enjoined from further infringement.

66. Comerica has had actual knowledge of the 802 Patent at least as of October 18, 2013, when Textile sent a letter to Ralph W. Babb, Jr., then Chief Executive Officer of Comerica Bank, that described certain implementations of the patented technology and specifically identified the 802 Patent.

67. Comerica has had actual knowledge of the 802 Patent at least as of November 10, 2014, when Textile sent a letter to Ralph W. Babb, Jr., then Chief Executive Officer of Comerica

Bank, that described certain implementations of the patented technology and specifically identified the 802 Patent.

68. Comerica has had actual knowledge of the 802 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Comerica will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 802 Patent.

69. Comerica has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 802 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

70. Textile has been damaged as a result of the infringing conduct by Comerica alleged above. Thus, Comerica is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

71. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 802 Patent.

COUNT III

INFRINGEMENT OF U.S. PATENT NO. 9,584,499

72. On February 28, 2017, United States Patent No. 9,584,499 (“the 499 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

73. Textile is the owner of the 499 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 499 Patent against infringers, and to collect damages for all relevant times.

74. Comerica offers debit and/or credit cards, such as the Comerica Debit Mastercard, that are used by Comerica in practicing a method for authorizing transaction specific access to a secured resource having a secured resource identity (the “Accused Instrumentality”). The Comerica transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.

Comerica

Personal Small Business Commercial Wealth Management

Banking Borrowing Investing Insurance

Home > Personal > Banking > Online Services > Mobile Wallet

Mobile Wallets

Your mobile device, your mobile wallet

Pay with your Comerica debit or credit card using your preferred mobile wallet.

Use your Comerica debit and credit card on Apple Pay®, Samsung Pay and Google Pay™ to make checkouts at your favorite retailers convenient, fast, and secure. Pay confidently from your mobile device knowing that the same fraud protection Comerica gives your credit and debit card carries over to your mobile wallet.

With a simple tap, click or touch, you can shop with ease in-store, online, and in-app.

In-store purchases:

Stop fumbling for your wallet. Pay with your mobile device wherever you see the contactless payment symbol at checkout.

Online and in-app purchases:

Rather than entering your credit or debit card number and address details, select your mobile wallet where accepted when shopping online and in-app to save time.

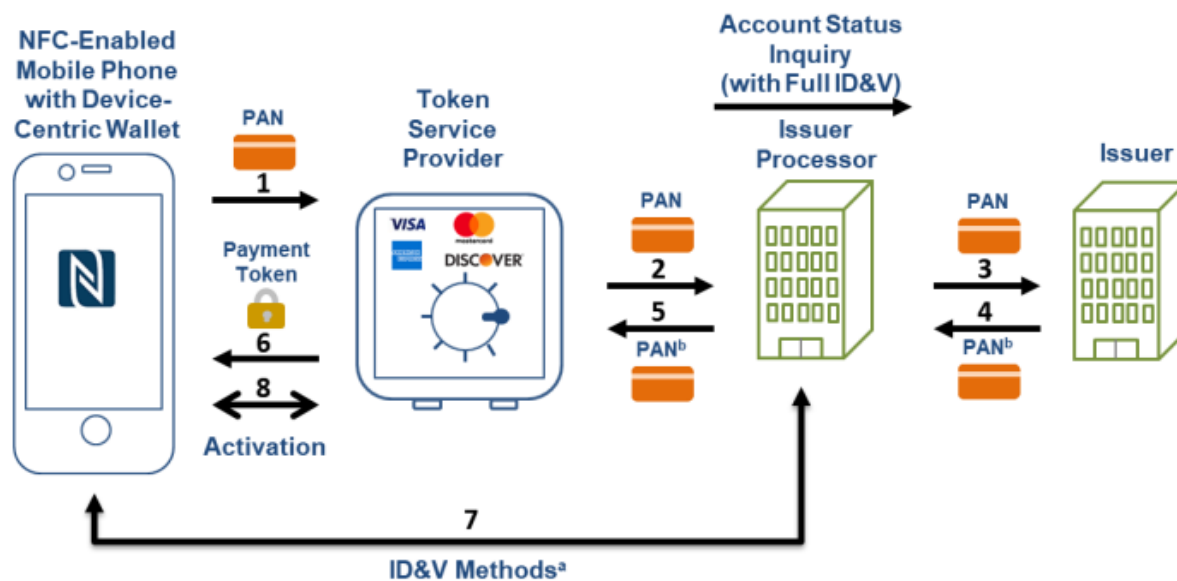
Select your mobile wallet below to learn how to add your Comerica credit or debit card, and change the way you pay today!

Click a logo below to learn more.

(Source: <https://www.comerica.com/personal-finance/banking/online-services/mobile-wallet.html>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

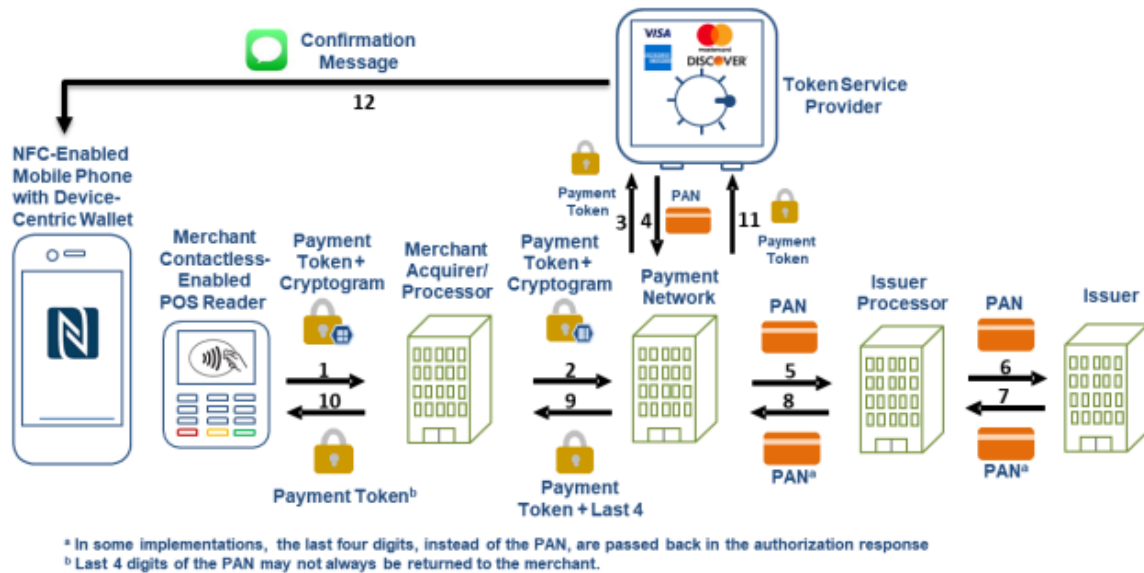


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

75. Comerica's use of the Accused Instrumentality includes a method for authorizing transaction specific access to a secured resource having a secured resource identity. For example, a Comerica account holder requests Comerica to provision a specific Comerica debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Comerica card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's

smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram.

76. The Accused Instrumentality includes receiving at a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive a request for transaction specific access to a secured resource by a service client. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Comerica card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Comerica card account of the account holder. This messaging gateway is either hosted directly by Comerica or through an agent with whom Comerica has contracted to receive the messages.

77. The Accused Instrumentality includes generating a key string with a server in communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate the key string known to both said server and an authorized user of the secured resource, said key string being associated with the secured resource within a key string table accessible by the server and providing a basis for authenticating the secured resource identity by searching the key string table for the key string. For example, behind the firewall of the messaging gateway and in communication therewith is an authorization server that generates a token corresponding to a secured resource during the

provisioning process. After this, the authorization server updates a table that maps token numbers to secured resource identities. The authorization server is then able to search the table to authenticate a secured resource identity by searching the table for the token. If the token has a corresponding secured resource identity, that identity is authenticated. The authorization server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to provide the authentication services.

78. The Accused Instrumentality includes determining transaction specific information with the server in communication with the messaging gateway, the server having a third set of instructions embodied in a computer readable medium operable to identify transaction specific information within the request. For example, the authorization server is also programmed to identify within the payment authorization request transaction specific information that was passed by the merchant. The authorization server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to provide the authentication services.

79. The Accused Instrumentality includes communicating said key string to said authorized user. For example, once the provisioning process is complete, the messaging gateway and/or the server send the token to the authorized user's mobile device. The messaging gateway is either hosted directly by Comerica or through an agent with whom Comerica has contracted to provide the authentication services. The authorization server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to provide the authentication services.

80. The Accused Instrumentality includes receiving an authentication credential from said service client, said authentication credential having been provided to said service client by

said authorized user. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant. The authorization server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to provide the authentication services.

81. The Accused Instrumentality includes evaluating said authentication credential. For example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authorizes the transaction specific access. The authorization server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to provide the authentication services.

82. The Accused Instrumentality includes wherein the key string and authentication credential do not reveal any primary identifier associated with said secured resource. For example, neither the token nor the cryptogram reveals the debit and/or credit card number associated with the secured resource.

83. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

84. Defendants thus infringe one or more claims of the 499 Patent. The elements and conduct described herein are covered by and infringe upon at least Claim 3 of the 499 Patent.

Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 499 Patent.

85. Comerica has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

86. Comerica has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 499 Patent by others and Comerica will continue to do so unless enjoined by this Court. Comerica's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 499 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Comerica knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 499 Patent.

87. Comerica continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers,

businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 499 Patent.

88. Comerica has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 499 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

89. Comerica has committed these acts of infringement without license or authorization.

90. By engaging in the conduct described herein, Comerica has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Comerica is thus liable to Textile for infringement of the 499 Patent, pursuant to 35 U.S.C. § 271.

91. As a direct and proximate result of Comerica's infringement of the 499 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Comerica's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

92. In addition, the infringing acts and practices of Comerica have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Comerica is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Comerica is finally and permanently enjoined from further infringement.

93. Comerica has had actual knowledge of the 499 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Comerica will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 499 Patent.

94. Comerica has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 499 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

95. Textile has been damaged as a result of the infringing conduct by Comerica alleged above. Thus, Comerica is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

96. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 499 Patent.

COUNT IV

INFRINGEMENT OF U.S. PATENT NO. 10,148,659

97. On December 4, 2018, United States Patent No. 10,148,659 (“the 659 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

98. Textile is the owner of the 659 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 659 Patent against infringers, and to collect damages for all relevant times.

99. Comerica offers debit and/or credit cards, such as the Comerica Debit Mastercard, that are used with a computer-implemented system for a credit or debit and/or credit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit and/or credit card account number to the merchant (the “Accused Instrumentality”). The Comerica transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.

Comerica

Personal

Small Business

Commercial

Wealth Management

Banking

Borrowing

Investing

Insurance

[Home](#) > [Personal](#) > [Banking](#) > [Online Services](#) > Mobile Wallet

Mobile Wallets

Your mobile device, your mobile wallet


Pay with your Comerica debit or credit card using your preferred mobile wallet.

Use your Comerica debit and credit card on Apple Pay®, Samsung Pay and Google Pay™ to make checkouts at your favorite retailers convenient, fast, and secure. Pay confidently from your mobile device knowing that the same fraud protection Comerica gives your credit and debit card carries over to your mobile wallet.

With a simple tap, click or touch, you can shop with ease in-store, online, and in-app.


In-store purchases:

Stop fumbling for your wallet. Pay with your mobile device wherever you see the contactless payment symbol at checkout.



Online and in-app purchases:

Rather than entering your credit or debit card number and address details, select your mobile wallet where accepted when shopping online and in-app to save time.



failing for up.pxivlad...

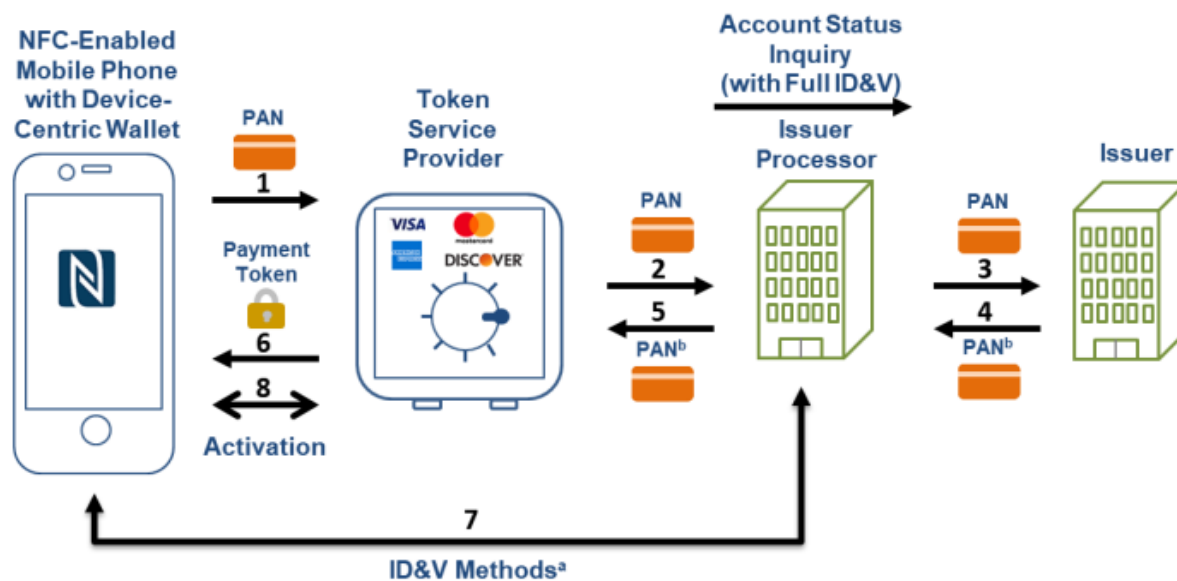
Select your mobile wallet below to learn how to add your Comerica credit or debit card, and change the way you pay today!

Click a logo below to learn more.

(Source: <https://www.comerica.com/personal-finance/banking/online-services/mobile-wallet.html>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

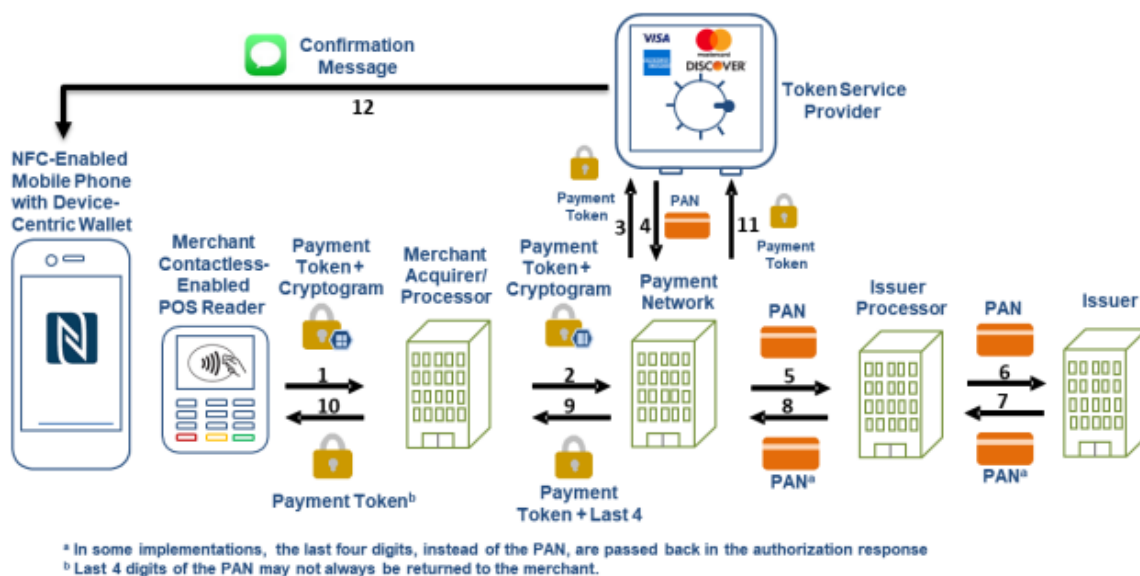


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

100. The Accused Instrumentality includes a computer-implemented system for a credit or debit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit card account number to the merchant. For example, a Comerica account holder requests Comerica to provision a specific Comerica debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Comerica to a specific merchant in a specific amount for a specific transaction from a specific

Comerica card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

101. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a credit or debit card account holder's mobile device, a merchant's payment application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a Comerica card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Comerica card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Comerica card account of the account holder. This interface is either hosted directly by Comerica or through an agent with whom Comerica has contracted to receive the messages.

102. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration

information received from the credit or debit card account holder through the at least one interface, the registration information comprising a credit or debit card account holder identifier and at least one credit or debit card account number having an associated unique account identifier wherein the credit or debit card account number and unique account identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card and the debit and/or credit card account number (which has a corresponding token), received from Comerica card account holders through the interface for provisioning a specific Comerica debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Comerica card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Comerica card account of the account holder. The server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to receive the messages.

103. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to pay the specific merchant for the specific transaction from a given debit or credit card account, the authorization request message having been received through the at least one interface and originating from the credit or debit card account holder's mobile device and comprising: a first merchant identifier; a first transaction specific information selected from the group consisting of a first transaction amount and first client reference identifier; the credit or debit card account holder identifier; and a designated unique account identifier selected from the at least one unique account identifiers. For example, the Accused

Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Comerica card account holder's mobile device. The server is programmed to receive authorization requests initiated by Comerica card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a merchant identifier, and the Comerica card account holder identifier. The server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to receive the messages.

104. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string wherein the key string is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the designated unique account identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to receive the messages.

105. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive a payment request message from the merchant's payment application through the at least one interface, the payment request message comprising: a second merchant identifier; a second transaction specific information selected from the group consisting of a second transaction amount and second client reference identifier; and a second transaction specific authentication credential whereby the second authentication credential was received by the merchant application from the credit or debit card account holder's mobile device. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Comerica card account holder's mobile device. The server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to receive the messages.

106. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the credit or debit card account holder's request to use the credit or debit card account number associated with the designated unique account identifier for payment to the specific merchant for the specific transaction and authorizing the resource provider to use the credit or debit card account number associated with the designated unique account identifier to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or bank account number to the

specific merchant by determining if: the first merchant identifier matches the second merchant identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to provide the authentication services.

107. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

108. Defendants thus infringe one or more claims of the 659 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 9 of the 659 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 659 Patent.

109. Comerica has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C.

§ 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

110. Comerica has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 659 Patent by others and Comerica will continue to do so unless enjoined by this Court. Comerica's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 659 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Comerica knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 659 Patent.

111. Comerica continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 659 Patent.

112. Comerica has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 9 of the 659 Patent, in violation of 35 U.S.C.

§ 271(c), by contributing to the direct infringement of the 659 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

113. Comerica has committed these acts of infringement without license or authorization.

114. By engaging in the conduct described herein, Comerica has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Comerica is thus liable to Textile for infringement of the 659 Patent, pursuant to 35 U.S.C. § 271.

115. As a direct and proximate result of Comerica's infringement of the 659 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Comerica's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

116. In addition, the infringing acts and practices of Comerica have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Comerica is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such,

Textile is entitled to compensation for any continuing and/or future infringement up until the date that Comerica is finally and permanently enjoined from further infringement.

117. Comerica has had actual knowledge of the 659 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Comerica will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 659 Patent.

118. Comerica has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 659 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

119. Textile has been damaged as a result of the infringing conduct by Comerica alleged above. Thus, Comerica is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

120. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 659 Patent.

COUNT V

INFRINGEMENT OF U.S. PATENT NO. 10,560,454

121. On February 11, 2020, United States Patent No. 10,560,454 (“the 454 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

122. Textile is the owner of the 454 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 454 Patent against infringers, and to collect damages for all relevant times.

123. Comerica offers debit and/or credit cards, such as the Comerica Debit Mastercard, that are used with a computer-implemented system for a user to authorize a resource authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client (the "Accused Instrumentality"). The Comerica transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.

Comerica

Personal Small Business Commercial Wealth Management

Banking Borrowing Investing Insurance

Home > Personal > Banking > Online Services > Mobile Wallet

Mobile Wallets

Your mobile device, your mobile wallet

Pay with your Comerica debit or credit card using your preferred mobile wallet.

Use your Comerica debit and credit card on Apple Pay®, Samsung Pay and Google Pay™ to make checkouts at your favorite retailers convenient, fast, and secure. Pay confidently from your mobile device knowing that the same fraud protection Comerica gives your credit and debit card carries over to your mobile wallet.

With a simple tap, click or touch, you can shop with ease in-store, online, and in-app.

In-store purchases:

Stop fumbling for your wallet. Pay with your mobile device wherever you see the contactless payment symbol at checkout.

Online and in-app purchases:

Rather than entering your credit or debit card number and address details, select your mobile wallet where accepted when shopping online and in-app to save time.

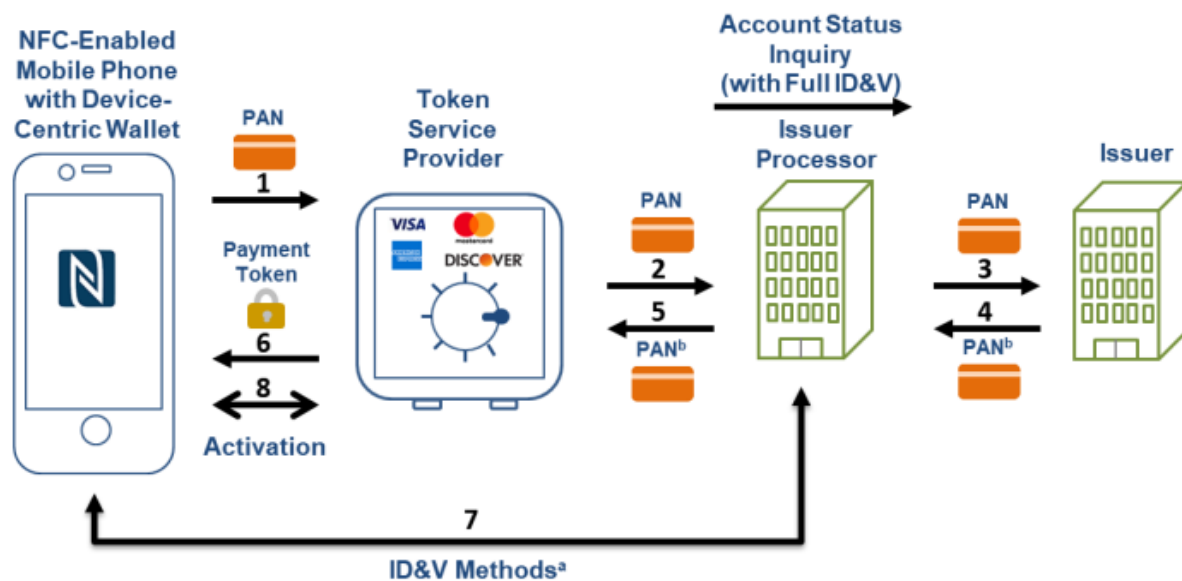
Select your mobile wallet below to learn how to add your Comerica credit or debit card, and change the way you pay today!

Click a logo below to learn more.

(Source: <https://www.comerica.com/personal-finance/banking/online-services/mobile-wallet.html>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

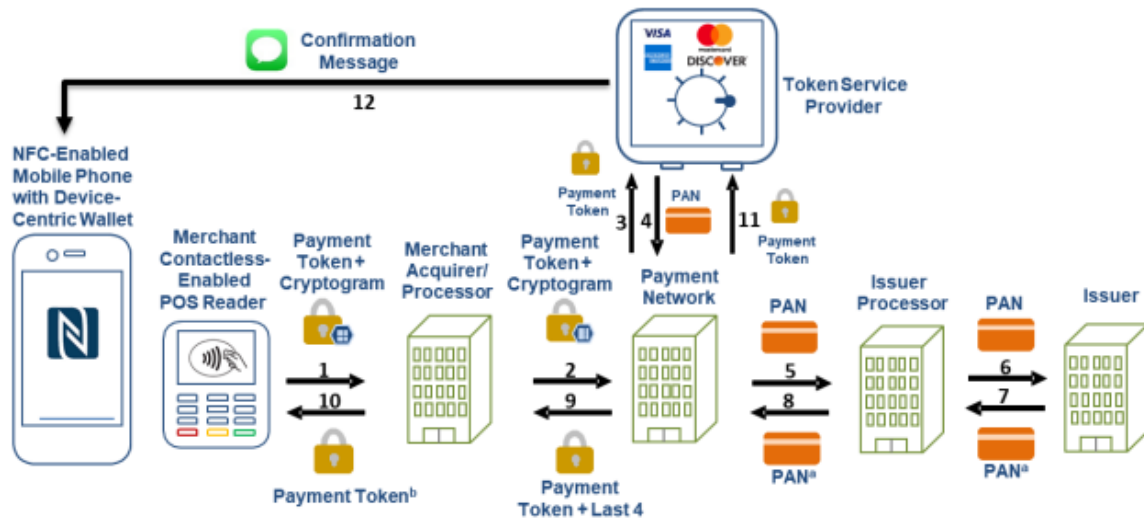
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

124. The Accused Instrumentality includes a computer-implemented system for a user to authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client. For example, a Comerica account holder requests Comerica to provision a specific Comerica debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Comerica to a specific merchant in a specific amount for a specific transaction from a specific Comerica card account of the account holder

using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

125. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a user's application, a service client's application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a Comerica card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Comerica card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Comerica card account of the account holder. This interface is either hosted directly by Comerica or through an agent with whom Comerica has contracted to receive the messages.

126. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration information received from the user through the at least one interface, the registration information comprising a user identifier and at least one secured resource identifier associated with the

common identifier of the secured resource, wherein the common identifier and secured resource identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card, the debit and/or credit card account number (which has a corresponding token), and the CVV number received from Comerica card account holders through the interface for provisioning a specific Comerica debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Comerica card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Comerica card account of the account holder. The server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to receive the messages.

127. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to authorize access to the secured resource by the service client, the authorization request message having been received through the at least one interface from the user's application and comprising: a first service client identifier; a first transaction specific information; the user identifier; and a designated secured resource identifier selected from one of the at least one secured resource identifiers. For example, the Accused Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Comerica card account holder's mobile device. The server is programmed to receive authorization requests initiated by Comerica card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction,

a token, a CVV number, a merchant identifier, other token information, and the Comerica card account holder identifier. The server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to receive the messages.

128. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string and does not include or reveal the common identifier associated with the designated secured resource identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to receive the messages.

129. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive an access request message from the service client's application through the at least one interface, the payment request message comprising: a second service client identifier; a second transaction specific information; and a second transaction specific authentication credential whereby the second transaction specific authentication credential was received by the service client's

application from the user's application. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Comerica card account holder's mobile device. The server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to receive the messages.

130. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the user's request to access the secured resource associated with the designated secured resource identifier without transmitting or otherwise providing the common identifier of the secured resource to the service client by determining if: the first service client identifier matches the second service client identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Comerica or through an agent with whom Comerica has contracted to provide the authentication services.

131. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

132. Defendants thus infringe one or more claims of the 454 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 8 of the 454 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 454 Patent.

133. Comerica has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

134. Comerica has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 454 Patent by others and Comerica will continue to do so unless enjoined by this Court. Comerica's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for

another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 454 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Comerica knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 454 Patent.

135. Comerica continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 454 Patent.

136. Comerica has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 454 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

137. Comerica has committed these acts of infringement without license or authorization.

138. By engaging in the conduct described herein, Comerica has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Comerica is thus liable to Textile for infringement of the 454 Patent, pursuant to 35 U.S.C. § 271.

139. As a direct and proximate result of Comerica's infringement of the 454 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Comerica's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

140. In addition, the infringing acts and practices of Comerica have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Comerica is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Comerica is finally and permanently enjoined from further infringement.

141. Comerica has had actual knowledge of the 454 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Comerica will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 454 Patent.

142. Comerica has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 454 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

143. Textile has been damaged as a result of the infringing conduct by Comerica alleged above. Thus, Comerica is liable to Textile in an amount that adequately compensates it

for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

144. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 454 Patent.

ADDITIONAL ALLEGATIONS REGARDING INFRINGEMENT

145. Comerica has also indirectly infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by inducing others to directly infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Comerica has induced the end-users, Comerica's customers, to directly infringe (literally and/or under the doctrine of equivalents) the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by using the Accused Instrumentality.

146. Comerica took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

147. Such steps by Comerica included, among other things, advising or directing customers and end-users to use the Accused Instrumentality in an infringing manner; advertising and promoting the use of the Accused Instrumentality in an infringing manner; and/or distributing instructions that guide users to use the Accused Instrumentality in an infringing manner.

148. Comerica has performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454

Patent and with the knowledge that the induced acts constitute infringement, at least since the filing of the Complaint.

149. Comerica was and is aware that the normal and customary use of the Accused Instrumentality by Comerica's customers would infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Comerica's inducement is ongoing.

150. Comerica directs or controls the use of the Accused Instrumentality nationwide through its own websites and in its own branches, including in Texas and elsewhere in the United States, and expects and intends that the Accused Instrumentality will be so used.

151. Comerica took active steps, directly and/or through contractual relationships with others, with the specific intent to cause such persons to make or use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

152. Comerica performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts would constitute infringement.

153. Comerica's inducement is ongoing.

154. Comerica has also indirectly infringed by contributing to the infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Comerica has contributed to the direct infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by the end-user of the Accused Instrumentality.

155. The Accused Instrumentality has special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the 079

Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

156. As described above, the special features include securely authorizing specific transactions without providing a credit or debit card number to the merchant used in a manner that infringes the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

157. The special features constitute a material part of the invention of one or more of the claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and are not staple articles of commerce suitable for substantial non-infringing use.

158. Comerica's contributory infringement is ongoing.

159. Comerica's actions are at least objectively reckless as to the risk of infringing valid patents and this objective risk was either known or should have been known by Comerica, at least since the filing of the Complaint.

160. Comerica has had knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent at least since the filing of the Complaint.

161. Comerica's customers have infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

162. Comerica encouraged its customers' infringement.

163. Comerica's direct and indirect infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent is, has been, and/or continues to be willful, intentional, deliberate, and/or in conscious disregard of Textile's rights under the patents.

164. Textile has been damaged as a result of the infringing conduct by Comerica alleged above. Thus, Comerica is liable to Textile in an amount that adequately compensates it

for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Textile hereby requests a trial by jury on all issues so triable by right.

PRAYER FOR RELIEF

Textile requests that the Court find in its favor and against Comerica, and that the Court grant Textile the following relief:

- a. Judgment that one or more claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent have been infringed, either literally and/or under the doctrine of equivalents, by Comerica and/or all others acting in concert therewith;
- b. A permanent injunction enjoining Comerica and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert therewith from infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent; or, in the alternative, an award of a reasonable ongoing royalty for future infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by such entities;
- c. Judgment that Comerica account for and pay to Textile all damages to and costs incurred by Textile because of Comerica's infringing activities and other conduct complained of herein, including an award of all increased damages to which Textile is entitled under 35 U.S.C. § 284;
- d. That Textile be granted pre-judgment and post-judgment interest on the damages caused by Comerica's infringing activities and other conduct complained of herein;
- e. That this Court declare this an exceptional case and award Textile its reasonable

attorney's fees and costs in accordance with 35 U.S.C. § 285; and

f. That Textile be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: October 12, 2021

Respectfully submitted,

/s/ Matthew J. Antonelli

Matthew J. Antonelli

Texas Bar No. 24068432

matt@ahtlawfirm.com

Zachariah S. Harrington

Texas Bar No. 24057886

zac@ahtlawfirm.com

Larry D. Thompson, Jr.

Texas Bar No. 24051428

larry@ahtlawfirm.com

Christopher Ryan Pinckney

Texas Bar No. 24067819

ryan@ahtlawfirm.com

ANTONELLI, HARRINGTON

& THOMPSON LLP

4306 Yoakum Blvd., Ste. 450

Houston, TX 77006

(713) 581-3000

Stafford Davis

State Bar No. 24054605

sdavis@stafforddavisfirm.com

Catherine Bartles

Texas Bar No. 24104849

cbartles@stafforddavisfirm.com

THE STAFFORD DAVIS FIRM

815 South Broadway Avenue

Tyler, Texas 75701

(903) 593-7000

(903) 705-7369 fax

Of Counsel:

Sandeep Seth

Texas State Bar No. 18043000

SETHLAW

Pennzoil Place

700 Milam Street, Suite 1300

Houston, Texas 77002
Telephone: (713) 244-5017
ss@sethlaw.com

Attorneys for Textile Computer Systems, Inc.

EXHIBIT 2D

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

TEXTILE COMPUTER SYSTEMS, INC.,

Plaintiff,

v.

FROST BANK,

Defendant.

CIVIL ACTION NO. 6:21-cv-1053

ORIGINAL COMPLAINT FOR
PATENT INFRINGEMENT

JURY TRIAL DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Textile Computer Systems, Inc. (“Textile” or “Plaintiff”) files this original complaint against Defendant Frost Bank (“Frost”), alleging, based on its own knowledge as to itself and its own actions and based on information and belief as to all other matters, as follows:

PARTIES

1. Textile Computer Systems, Inc. is a corporation formed under the laws of the State of Texas, with a place of business at 618 Bluff Trail, San Antonio, Texas, 78216.
2. Frost Bank is a bank organized and existing under the laws of Texas. Frost Bank has its headquarters at 111 West Houston Street, San Antonio, Texas 78205.
3. Frost and its affiliates lead and are part of an interrelated group of companies which together comprise one of the country’s largest banking and financial service entities, including under the Frost brand.
4. Frost and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

5. Frost and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

6. Frost and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

7. Thus, Frost and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

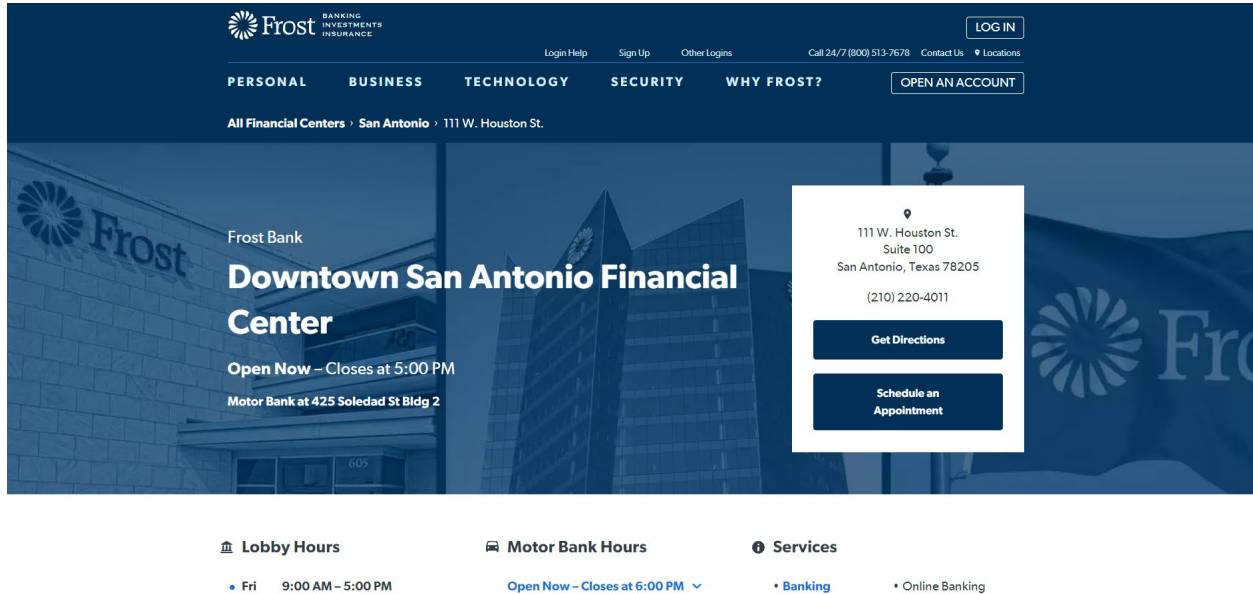
JURISDICTION AND VENUE

8. This is an action for infringement of United States patents arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. § 1331 and § 1338(a).

9. This Court has personal jurisdiction over Frost pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Frost has done and continues to do business in Texas; and (ii) Frost has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations, inducing others to commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein.

10. Venue is proper in this district pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Frost has committed and continues to commit acts of patent infringement in this district. For example, Frost cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those cardholders make

and/or use the accused instrumentalities in the district. Frost induces others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. Frost has regular and established places of business in this district, including at least at 111 W. Houston St., San Antonio, Texas 78205 and at numerous other locations in San Antonio and Austin:



(Source: <https://locations.frostbank.com/san-antonio/111-w.-houston-st.>)



(Source: screenshot from Google Maps Street View)

BACKGROUND

11. The patents-in-suit generally pertain to payment authorization technology used in payment networks used to process transactions from, for example, credit cards and debit cards. The technology disclosed by the patents was developed by Gopal Nandakumar, a Texas-based entrepreneur, software engineer, and prolific inventor with over 30 years of experience in the field of Information Management Systems.

12. In 1987, after receiving Master's Degrees from both the University of Madras, India and the Georgia Institute of Technology, Mr. Nandakumar formed Textile Computer Systems, Inc. ("Textile") for the purpose of consulting and developing software for the textile industry. In 2005, Textile began transitioning into credit card transaction systems. In 2011, Textile began to develop and market the MySingleLink suite of applications.

13. The Nandakumar patents are related to payment authorization technology. Mr. Nandakumar has been at the forefront of payment authorization, developing, disclosing, and patenting solutions for reducing fraud in credit and debit card transactions. Indeed, the Nandakumar patents (or the applications leading to them) have been cited during patent prosecution over a hundred times, including by numerous leading companies in the payment authorization industry such as ADP, Bank of America, Google, Groupon, IBM, Mastercard, NEC, Paypal, Visa, and Wells Fargo.

THE TECHNOLOGY

14. The patents-in-suit, U.S. Patent Nos. 8,505,079, 8,533,802, 9,584,499, 10,148,659, and 10,560,454 (collectively, the "Asserted Patents"), teach systems, including payment processing systems, for securely and effectively approving and processing specific credit card and/or debit card transactions. Through the specific use of servers, messaging

gateways, and/or interfaces, these systems act to reduce credit card and/or debit card fraud and misuse through their use and validation of key strings, authentication credentials, transaction specific information, and transaction specific credentials. The technology in the Asserted Patents improves the underlying functionality of existing card processing infrastructure by minimizing fraud and data theft in the face of attacks on payment systems that continue to grow in their number and sophistication.

15. The patented improvements are critical for implementing secure payment systems, especially in light of the many high-profile merchant data breaches that have lead to increased credit and debit card fraud. For example, in 2006, TJX Companies, who owns retailers like TJMaxx and Marshall's, was hit with a cyber attack that resulted in the theft of credit cards leading to over \$100 million in fraud losses. In 2013, five people were indicted for attacking a number of retailers and financial institutions including NASDAQ, 7-Eleven, JCP, and others, stealing over 160 million cards. Also in 2013, the retailer Target suffered a data breach that resulted in 40 million debit and credit cards being compromised.

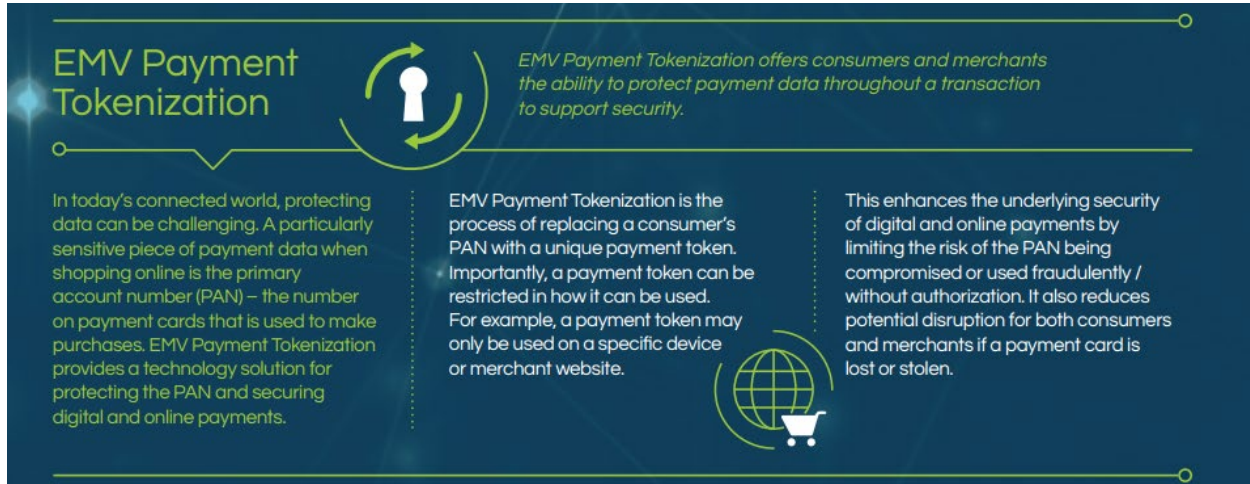
16. One implementation of the technology claimed in the Asserted Patents has been described by EMVCo as “a global Payment Tokenisation ecosystem that overlays and interoperates with existing payment ecosystems to support digital commerce and new methods of payment” and as “enhanc[ing] the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorized or fraudulent use of PANs.”

(Source: <https://www.emvco.com/emv-technologies/payment-tokenisation/>).

17. The technology claimed in the Asserted Patents is far from conventional technology. The payment industry gathered and consulted experts who worked together over a number of years to develop infringing payment tokenisation systems. In other words, the

technology claimed in the Asserted Patents was not existing or conventional technology that the payment industry had sitting on the shelf.

18. Indeed, as recently as February of this year, EMVCo itself recognized that an implementation of the technology claimed in the Asserted Patents “provides a technology solution for protecting the PAN and securing digital and online payments”:



(Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

19. That same EMVCo document notes that “In today’s connected world, protecting data can be challenging. A particularly sensitive piece of payment data when shopping online is the primary account number (PAN) – the number on payment cards that is used to make purchases” and that EMVCo’s payment tokenization “enhances the underlying security of digital and online payments by limiting the risk of the PAN being compromised or used fraudulently / without authorization.” The document also states that the “Payment Tokenisation Specification provides an interoperable Technical Framework.” (Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

20. One of the asserted patents, the 079 Patent, was challenged in an Inter Partes Review proceeding before the Patent and Trademark Office (“PTO”). The PTO found that the challenger, Unified Patents Inc., was unable to show that one element, the “key string” as claimed in the 079 Patent claims and as construed by the PTO, was in the prior art at all, much less it being conventional or widespread. The PTO thus confirmed the patentability of all challenged claims of the 079 Patent.

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 8,505,079

21. On August 6, 2013, United States Patent No. 8,505,079 (“the 079 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

22. Textile is the owner of the 079 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 079 Patent against infringers, and to collect damages for all relevant times.

23. Frost offers debit and/or credit cards, such as the Frost Visa Debit Card, that are used with an authentication system that authenticates the identity of a Frost card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Frost card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities, for example. The requests are initiated by account holders via their smartphones,

typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.

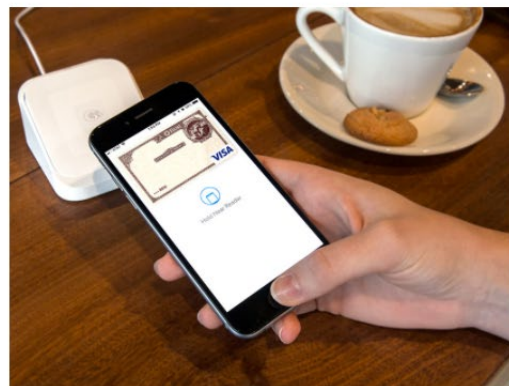


Digital Wallet

For Personal

No need to take your debit card out of your wallet. Simply make purchases using your smartphone, tablet or wearable — in stores, in apps and online. And because a device-specific number and unique transaction code is used, it's an even safer way to pay.

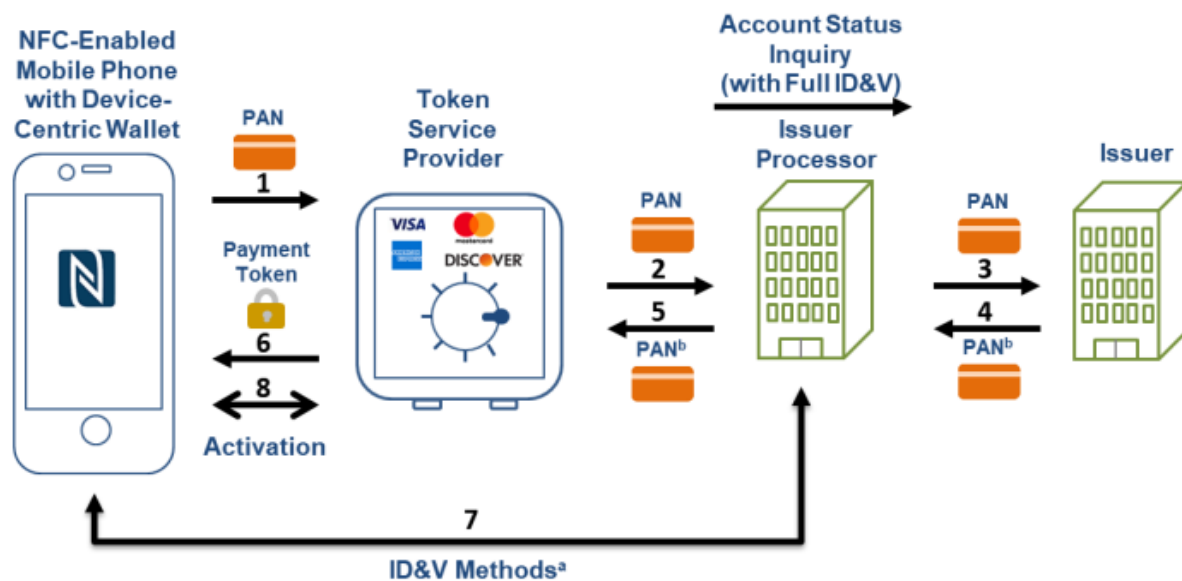
Available on Apple Pay[®], Google Pay[™], and Samsung Pay.



(Source: <https://www.frostbank.com/banking/financial-technology/>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

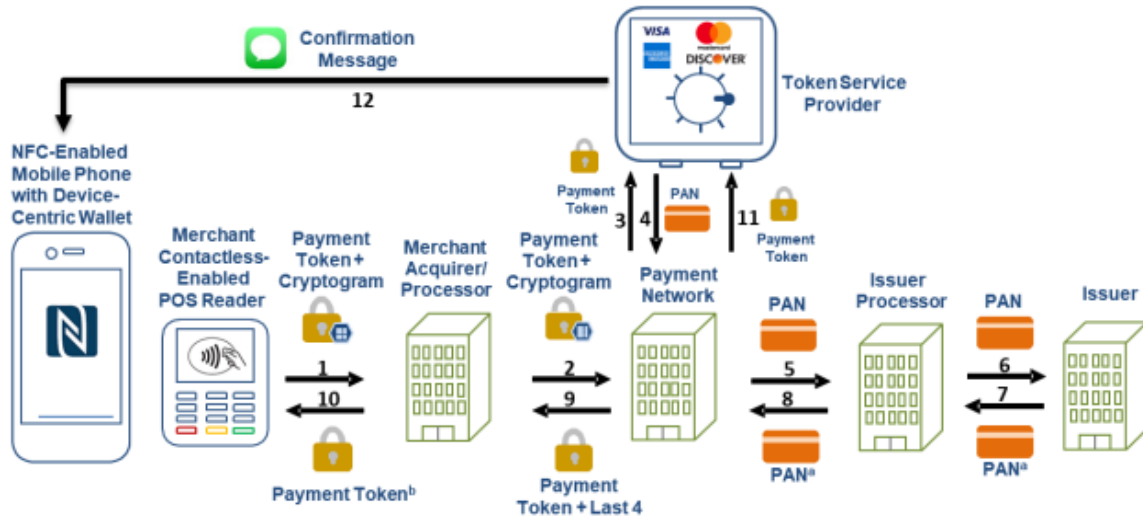
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

24. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a Frost account holder requests Frost to provision a specific Frost debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Frost card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives

certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

25. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Frost card account holders for provisioning a specific Frost debit and/or credit card for use on their mobile devices. The messaging gateway is also programmed to receive requests initiated by Frost card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Frost card account of the account holder. This messaging gateway is either hosted directly by Frost or through an agent with whom Frost has contracted to receive the messages.

26. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to determine a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the messaging

gateway and in secure communication therewith is an authorization server that processes the received request to identify the token value sent for the account selected to be charged that was passed from the authorized user to the merchant terminal via the NFC communication link. From the token value, the server can look up the debit and/or credit card account number. The authorization server is either hosted directly by Frost or through an agent with whom Frost has contracted to provide the authentication services.

27. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive within the payment authorization request transaction specific information that was input into the request by the merchant. The interface is either hosted directly by Frost or through an agent with whom Frost has contracted to provide the authentication services.

28. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

29. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

30. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

31. Defendants thus infringe one or more of the claims of the 079 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 079 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 079 Patent.

32. Frost has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(a), by making, using, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

33. Frost has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 079 Patent by others and Frost will continue to do so unless enjoined by this Court. Frost's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors,

agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 079 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Frost knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 079 Patent.

34. Frost continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 079 Patent.

35. Frost has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 079 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

36. Frost has committed these acts of infringement without license or authorization.

37. By engaging in the conduct described herein, Frost has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Frost is thus liable to Textile for infringement of the 079 Patent, pursuant to 35 U.S.C. § 271.

38. As a direct and proximate result of Frost's infringement of the 079 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Frost's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

39. In addition, the infringing acts and practices of Frost have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Frost is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Frost is finally and permanently enjoined from further infringement.

40. Frost has had actual knowledge of the 079 Patent at least as of October 18, 2013, when Textile sent a letter to Richard W. Evans, Jr., then Chief Executive Officer of Frost Bank, that described certain implementations of the patented technology and specifically identified the 079 Patent.

41. Frost has had actual knowledge of the 079 Patent at least as of November 10, 2014, when Textile sent a letter to Richard W. Evans, Jr., then Chief Executive Officer of Frost Bank, that described certain implementations of the patented technology and specifically identified the 079 Patent.

42. Frost has had actual knowledge of the 079 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Frost will have known and intended

(since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 079 Patent.

43. Frost has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 079 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

44. Textile has been damaged as a result of the infringing conduct by Frost alleged above. Thus, Frost is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

45. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 079 Patent.

COUNT II

INFRINGEMENT OF U.S. PATENT NO. 8,533,802

46. On September 10, 2013, United States Patent No. 8,533,802 (“the 802 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

47. Textile is the owner of the 802 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 802 Patent against infringers, and to collect damages for all relevant times.

48. Frost offers debit and/or credit cards, such as the Frost Visa Debit Card, that are used with an authentication system that authenticates the identity of a Frost card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Frost card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the

transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.

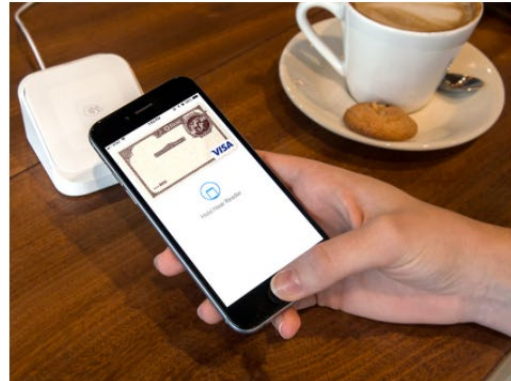


Digital Wallet

For Personal

No need to take your debit card out of your wallet. Simply make purchases using your smartphone, tablet or wearable — in stores, in apps and online. And because a device-specific number and unique transaction code is used, it's an even safer way to pay.

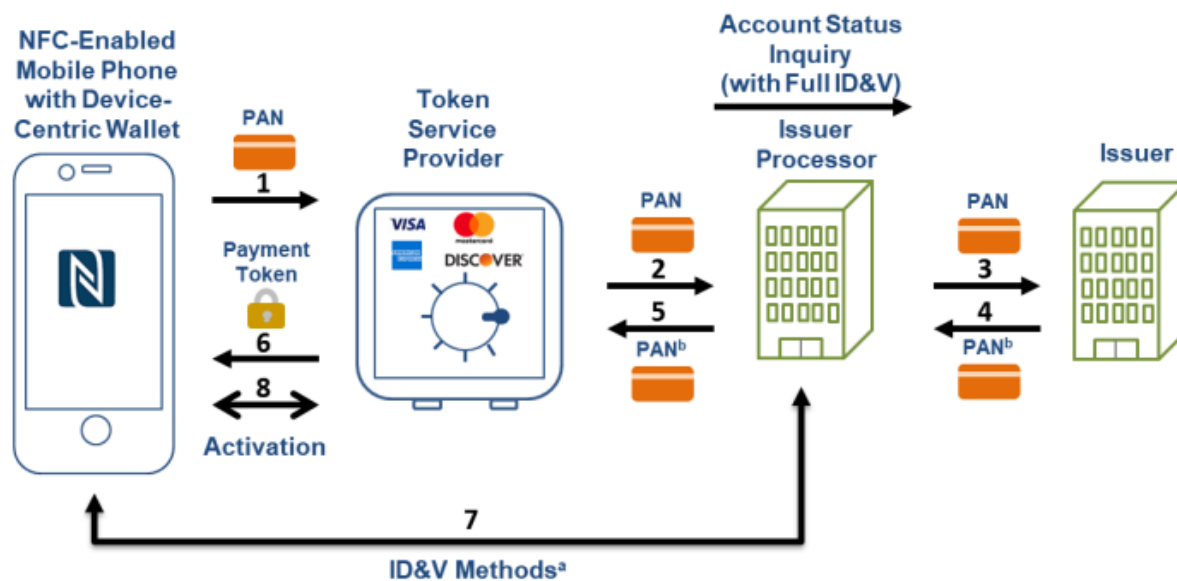
Available on Apple Pay[®], Google Pay[™], and Samsung Pay.



(Source: <https://www.frostbank.com/banking/financial-technology/>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

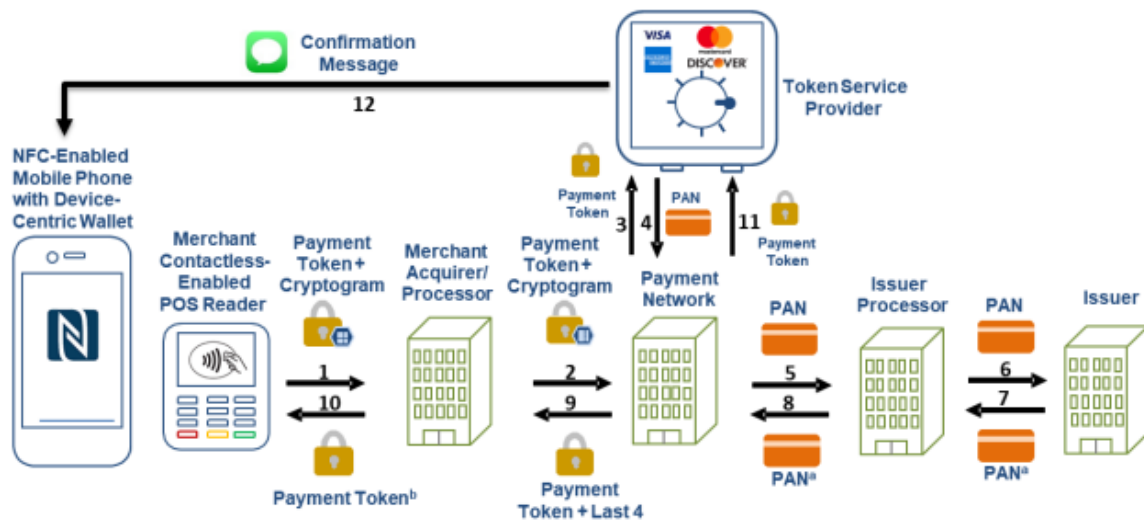
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response
^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

49. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a Frost account holder requests Frost to provision a specific Frost debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Frost card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives

certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

50. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Frost card account holders for provisioning a specific Frost debit and/or credit card for use on their mobile devices. This messaging gateway is either hosted directly by Frost or through an agent with whom Frost has contracted to receive the messages.

51. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate a key string adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the message gateway and in secure communication therewith is an authorization server that generates a token corresponding to the debit and/or credit card account number. The authorization server is either hosted directly by Frost or through an agent with whom Frost has contracted to provide the authentication services.

52. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive transaction specific information that was input into the request by the merchant, *e.g.*, the merchant ID, invoice number, invoice amount, and date/timestamp. The interface is either hosted directly by Frost or through an agent with whom Frost has contracted to provide the authentication services.

53. The Accused Instrumentality includes a first set of instructions further operable to communicate the key string to the authorized user that the requester purports to be. For example, the messaging gateway sends the generated token to the authorized user's mobile device for use in merchant transactions.

54. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

55. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

56. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

57. Defendants thus infringe one or more claims of the 802 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 802 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 802 Patents.

58. Frost has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

59. Frost has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 802 Patent by others and Frost will continue to do so unless enjoined by this Court. Frost's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors,

agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 802 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Frost knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 802 Patent.

60. Frost continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 802 Patent.

61. Frost has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 802 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

62. Frost has committed these acts of infringement without license or authorization.

63. By engaging in the conduct described herein, Frost has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Frost is thus liable to Textile for infringement of the 802 Patent, pursuant to 35 U.S.C. § 271.

64. As a direct and proximate result of Frost's infringement of the 802 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Frost's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

65. In addition, the infringing acts and practices of Frost have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Frost is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Frost is finally and permanently enjoined from further infringement.

66. Frost has had actual knowledge of the 802 Patent at least as of October 18, 2013, when Textile sent a letter to Richard W. Evans, Jr., then Chief Executive Officer of Frost Bank, that described certain implementations of the patented technology and specifically identified the 802 Patent.

67. Frost has had actual knowledge of the 802 Patent at least as of November 10, 2014, when Textile sent a letter to Richard W. Evans, Jr., then Chief Executive Officer of Frost Bank, that described certain implementations of the patented technology and specifically identified the 802 Patent.

68. Frost has had actual knowledge of the 802 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Frost will have known and intended

(since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 802 Patent.

69. Frost has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 802 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

70. Textile has been damaged as a result of the infringing conduct by Frost alleged above. Thus, Frost is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

71. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 802 Patent.

COUNT III

INFRINGEMENT OF U.S. PATENT NO. 9,584,499

72. On February 28, 2017, United States Patent No. 9,584,499 (“the 499 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

73. Textile is the owner of the 499 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 499 Patent against infringers, and to collect damages for all relevant times.

74. Frost offers debit and/or credit cards, such as the Frost Visa Debit Card, that are used by Frost in practicing a method for authorizing transaction specific access to a secured resource having a secured resource identity (the “Accused Instrumentality”). The Frost transaction-specific access authorization system is implemented, in part, via EMVCo compliant

tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.

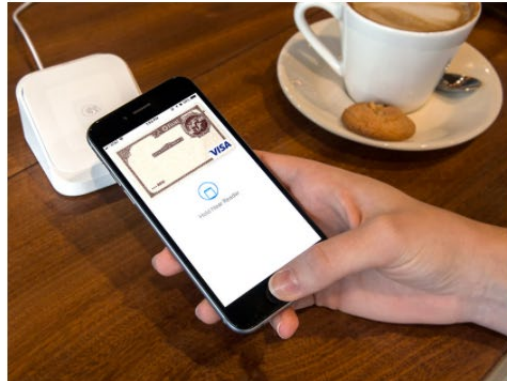


Digital Wallet

For Personal

No need to take your debit card out of your wallet. Simply make purchases using your smartphone, tablet or wearable — in stores, in apps and online. And because a device-specific number and unique transaction code is used, it's an even safer way to pay.

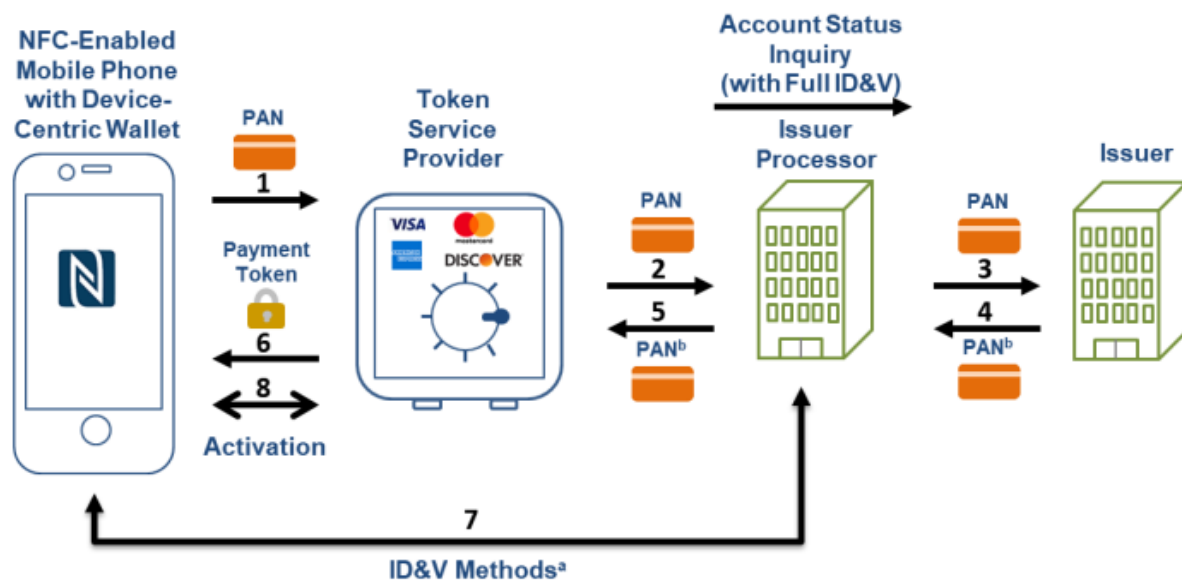
Available on Apple Pay[®], Google Pay[™], and Samsung Pay.



(Source: <https://www.frostbank.com/banking/financial-technology/>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

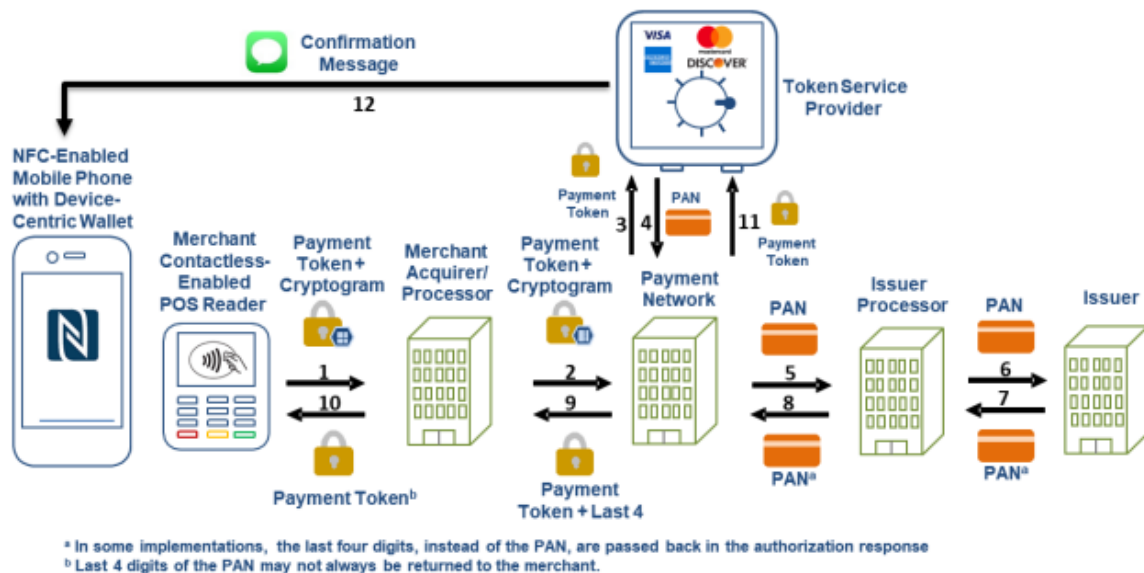


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

75. Frost's use of the Accused Instrumentality includes a method for authorizing transaction specific access to a secured resource having a secured resource identity. For example, a Frost account holder requests Frost to provision a specific Frost debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Frost card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives

certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram.

76. The Accused Instrumentality includes receiving at a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive a request for transaction specific access to a secured resource by a service client. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Frost card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Frost card account of the account holder. This messaging gateway is either hosted directly by Frost or through an agent with whom Frost has contracted to receive the messages.

77. The Accused Instrumentality includes generating a key string with a server in communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate the key string known to both said server and an authorized user of the secured resource, said key string being associated with the secured resource within a key string table accessible by the server and providing a basis for authenticating the secured resource identity by searching the key string table for the key string. For example, behind the firewall of the messaging gateway and in communication therewith is an authorization server that generates a token corresponding to a secured resource during the

provisioning process. After this, the authorization server updates a table that maps token numbers to secured resource identities. The authorization server is then able to search the table to authenticate a secured resource identity by searching the table for the token. If the token has a corresponding secured resource identity, that identity is authenticated. The authorization server is either hosted directly by Frost or through an agent with whom Frost has contracted to provide the authentication services.

78. The Accused Instrumentality includes determining transaction specific information with the server in communication with the messaging gateway, the server having a third set of instructions embodied in a computer readable medium operable to identify transaction specific information within the request. For example, the authorization server is also programmed to identify within the payment authorization request transaction specific information that was passed by the merchant. The authorization server is either hosted directly by Frost or through an agent with whom Frost has contracted to provide the authentication services.

79. The Accused Instrumentality includes communicating said key string to said authorized user. For example, once the provisioning process is complete, the messaging gateway and/or the server send the token to the authorized user's mobile device. The messaging gateway is either hosted directly by Frost or through an agent with whom Frost has contracted to provide the authentication services. The authorization server is either hosted directly by Frost or through an agent with whom Frost has contracted to provide the authentication services.

80. The Accused Instrumentality includes receiving an authentication credential from said service client, said authentication credential having been provided to said service client by said authorized user. For example, the authorization server is also programmed to identify within

the payment authorization request the cryptogram that was passed by the user to the merchant. The authorization server is either hosted directly by Frost or through an agent with whom Frost has contracted to provide the authentication services.

81. The Accused Instrumentality includes evaluating said authentication credential. For example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authorizes the transaction specific access. The authorization server is either hosted directly by Frost or through an agent with whom Frost has contracted to provide the authentication services.

82. The Accused Instrumentality includes wherein the key string and authentication credential do not reveal any primary identifier associated with said secured resource. For example, neither the token nor the cryptogram reveals the debit and/or credit card number associated with the secured resource.

83. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

84. Defendants thus infringe one or more claims of the 499 Patent. The elements and conduct described herein are covered by and infringe upon at least Claim 3 of the 499 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 499 Patent.

85. Frost has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

86. Frost has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 499 Patent by others and Frost will continue to do so unless enjoined by this Court. Frost's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 499 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Frost knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 499 Patent.

87. Frost continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 499 Patent.

88. Frost has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 499 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

89. Frost has committed these acts of infringement without license or authorization.

90. By engaging in the conduct described herein, Frost has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Frost is thus liable to Textile for infringement of the 499 Patent, pursuant to 35 U.S.C. § 271.

91. As a direct and proximate result of Frost's infringement of the 499 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Frost's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

92. In addition, the infringing acts and practices of Frost have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Frost is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is

entitled to compensation for any continuing and/or future infringement up until the date that Frost is finally and permanently enjoined from further infringement.

93. Frost has had actual knowledge of the 499 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Frost will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 499 Patent.

94. Frost has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 499 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

95. Textile has been damaged as a result of the infringing conduct by Frost alleged above. Thus, Frost is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

96. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 499 Patent.

COUNT IV

INFRINGEMENT OF U.S. PATENT NO. 10,148,659

97. On December 4, 2018, United States Patent No. 10,148,659 (“the 659 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

98. Textile is the owner of the 659 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 659 Patent against infringers, and to collect damages for all relevant times.

99. Frost offers debit and/or credit cards, such as the Frost Visa Debit Card, that are used with a computer-implemented system for a credit or debit and/or credit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit and/or credit card account number to the merchant (the “Accused Instrumentality”). The Frost transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.

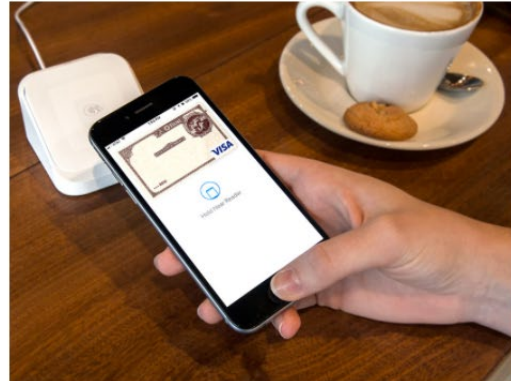


Digital Wallet

For Personal

No need to take your debit card out of your wallet. Simply make purchases using your smartphone, tablet or wearable — in stores, in apps and online. And because a device-specific number and unique transaction code is used, it's an even safer way to pay.

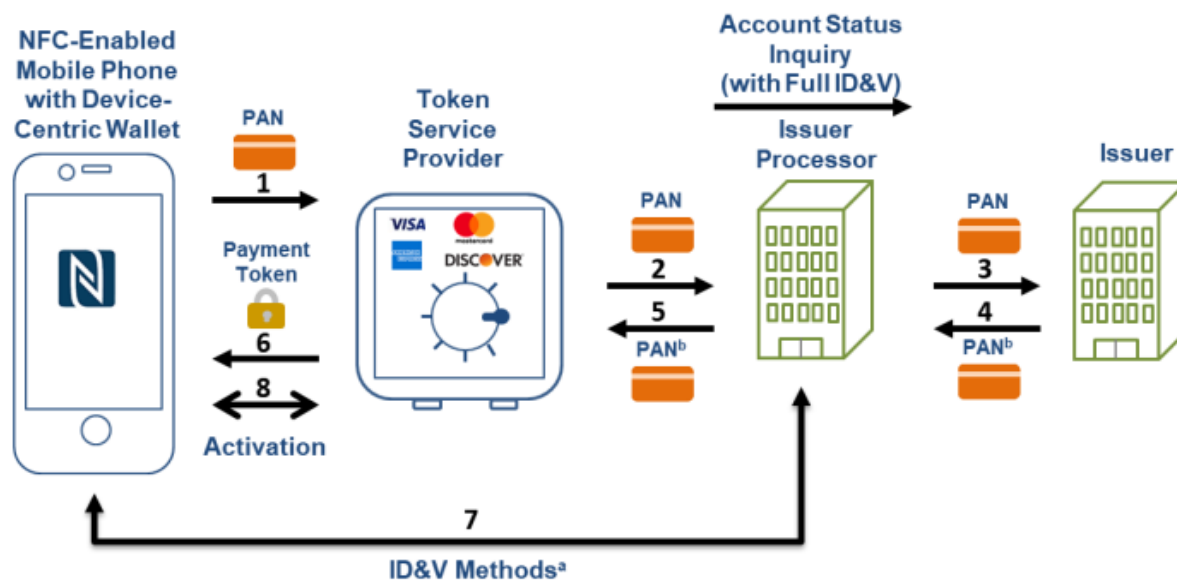
Available on Apple Pay[®], Google Pay[™], and Samsung Pay.



(Source: <https://www.frostbank.com/banking/financial-technology/>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

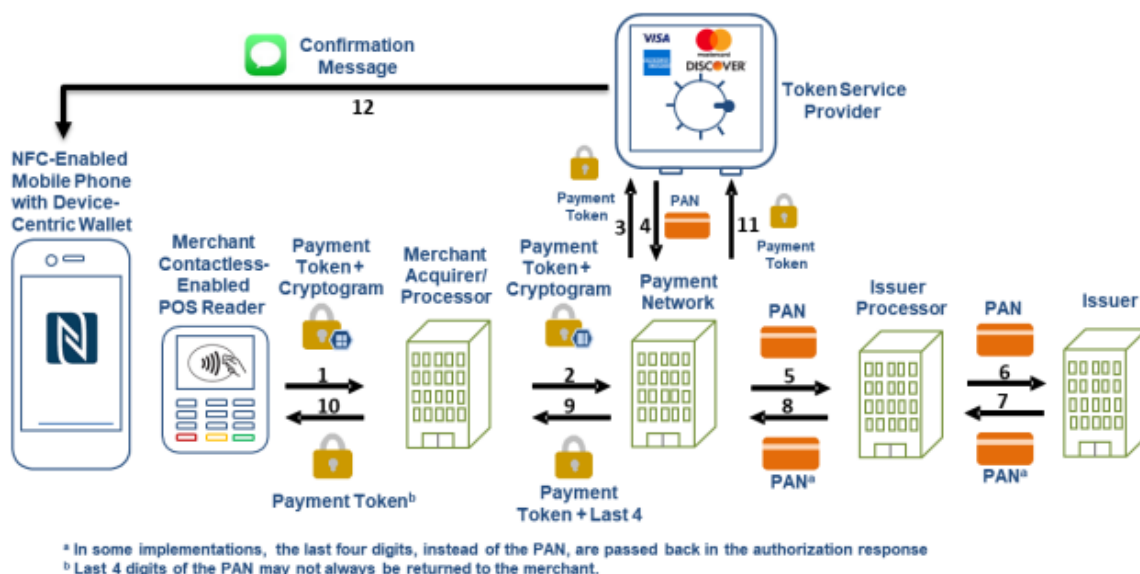


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

100. The Accused Instrumentality includes a computer-implemented system for a credit or debit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit card account number to the merchant. For example, a Frost account holder requests Frost to provision a specific Frost debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Frost to a specific merchant in a specific amount for a specific transaction from a specific Frost card

account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

101. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a credit or debit card account holder's mobile device, a merchant's payment application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a Frost card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Frost card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Frost card account of the account holder. This interface is either hosted directly by Frost or through an agent with whom Frost has contracted to receive the messages.

102. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration

information received from the credit or debit card account holder through the at least one interface, the registration information comprising a credit or debit card account holder identifier and at least one credit or debit card account number having an associated unique account identifier wherein the credit or debit card account number and unique account identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card and the debit and/or credit card account number (which has a corresponding token), received from Frost card account holders through the interface for provisioning a specific Frost debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Frost card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Frost card account of the account holder. The server is either hosted directly by Frost or through an agent with whom Frost has contracted to receive the messages.

103. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to pay the specific merchant for the specific transaction from a given debit or credit card account, the authorization request message having been received through the at least one interface and originating from the credit or debit card account holder's mobile device and comprising: a first merchant identifier; a first transaction specific information selected from the group consisting of a first transaction amount and first client reference identifier; the credit or debit card account holder identifier; and a designated unique account identifier selected from the at least one unique account identifiers. For example, the Accused

Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Frost card account holder's mobile device. The server is programmed to receive authorization requests initiated by Frost card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a merchant identifier, and the Frost card account holder identifier. The server is either hosted directly by Frost or through an agent with whom Frost has contracted to receive the messages.

104. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string wherein the key string is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the designated unique account identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Frost or through an agent with whom Frost has contracted to receive the messages.

105. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive a payment request message from the merchant's payment application through the at least one interface, the payment request message comprising: a second merchant identifier; a second transaction specific information selected from the group consisting of a second transaction amount and second client reference identifier; and a second transaction specific authentication credential whereby the second authentication credential was received by the merchant application from the credit or debit card account holder's mobile device. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Frost card account holder's mobile device. The server is either hosted directly by Frost or through an agent with whom Frost has contracted to receive the messages.

106. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the credit or debit card account holder's request to use the credit or debit card account number associated with the designated unique account identifier for payment to the specific merchant for the specific transaction and authorizing the resource provider to use the credit or debit card account number associated with the designated unique account identifier to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or bank account number to the

specific merchant by determining if: the first merchant identifier matches the second merchant identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Frost or through an agent with whom Frost has contracted to provide the authentication services.

107. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

108. Defendants thus infringe one or more claims of the 659 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 9 of the 659 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 659 Patent.

109. Frost has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. §

271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

110. Frost has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 659 Patent by others and Frost will continue to do so unless enjoined by this Court. Frost's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 659 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Frost knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 659 Patent.

111. Frost continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 659 Patent.

112. Frost has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 659 Patent by others, such as consumers,

businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

113. Frost has committed these acts of infringement without license or authorization.

114. By engaging in the conduct described herein, Frost has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Frost is thus liable to Textile for infringement of the 659 Patent, pursuant to 35 U.S.C. § 271.

115. As a direct and proximate result of Frost's infringement of the 659 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Frost's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

116. In addition, the infringing acts and practices of Frost have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Frost is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Frost is finally and permanently enjoined from further infringement.

117. Frost has had actual knowledge of the 659 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Frost will have known and intended

(since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 659 Patent.

118. Frost has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 659 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

119. Textile has been damaged as a result of the infringing conduct by Frost alleged above. Thus, Frost is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

120. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 659 Patent.

COUNT V

INFRINGEMENT OF U.S. PATENT NO. 10,560,454

121. On February 11, 2020, United States Patent No. 10,560,454 (“the 454 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

122. Textile is the owner of the 454 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 454 Patent against infringers, and to collect damages for all relevant times.

123. Frost offers debit and/or credit cards, such as the Frost Visa Debit Card, that are used with a computer-implemented system for a user to authorize a resource authorize a service client’s access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource’s common identifier to the service client (the “Accused

Instrumentality”). The Frost transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.

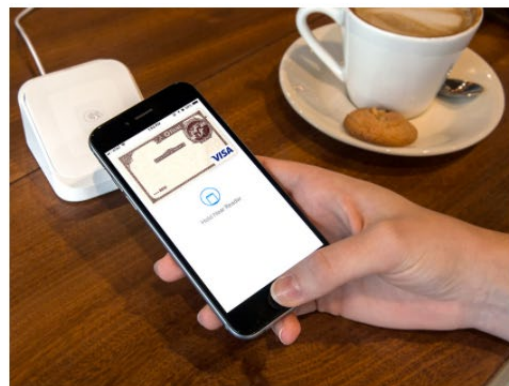


Digital Wallet

For Personal

No need to take your debit card out of your wallet. Simply make purchases using your smartphone, tablet or wearable — in stores, in apps and online. And because a device-specific number and unique transaction code is used, it's an even safer way to pay.

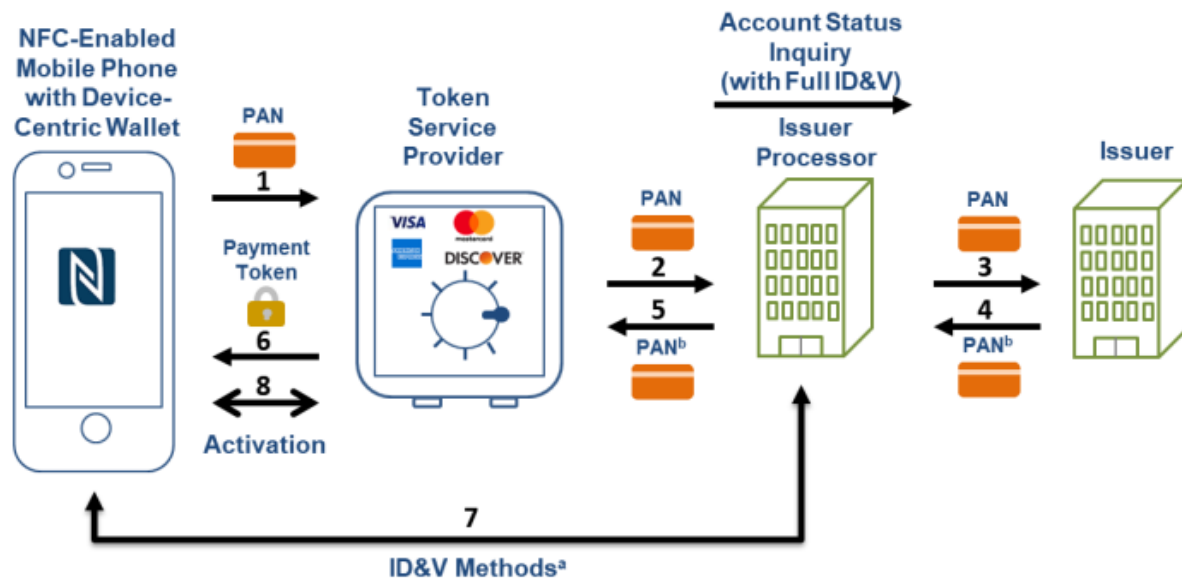
Available on Apple Pay®, Google Pay™, and Samsung Pay.



(Source: <https://www.frostbank.com/banking/financial-technology/>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

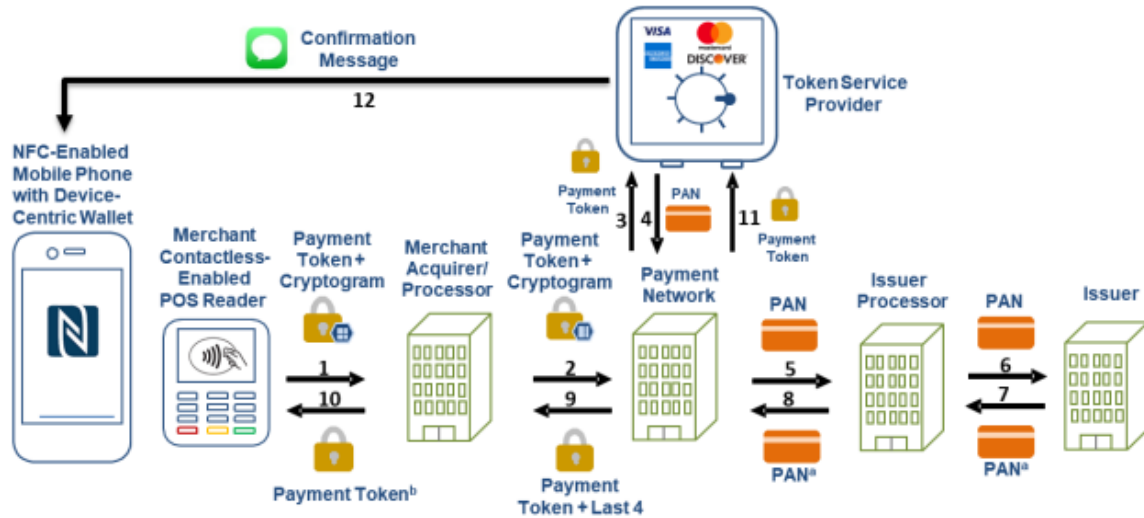
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

124. The Accused Instrumentality includes a computer-implemented system for a user to authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client. For example, a Frost account holder requests Frost to provision a specific Frost debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Frost to a specific merchant in a specific amount for a specific transaction from a specific Frost card account of the account holder using his or her smartphone

when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

125. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a user's application, a service client's application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a Frost card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Frost card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Frost card account of the account holder. This interface is either hosted directly by Frost or through an agent with whom Frost has contracted to receive the messages.

126. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration information received from the user through the at least one interface, the registration information comprising a user identifier and at least one secured resource identifier associated with the

common identifier of the secured resource, wherein the common identifier and secured resource identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card, the debit and/or credit card account number (which has a corresponding token), and the CVV number received from Frost card account holders through the interface for provisioning a specific Frost debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Frost card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Frost card account of the account holder. The server is either hosted directly by Frost or through an agent with whom Frost has contracted to receive the messages.

127. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to authorize access to the secured resource by the service client, the authorization request message having been received through the at least one interface from the user's application and comprising: a first service client identifier; a first transaction specific information; the user identifier; and a designated secured resource identifier selected from one of the at least one secured resource identifiers. For example, the Accused Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Frost card account holder's mobile device. The server is programmed to receive authorization requests initiated by Frost card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction,

a token, a CVV number, a merchant identifier, other token information, and the Frost card account holder identifier. The server is either hosted directly by Frost or through an agent with whom Frost has contracted to receive the messages.

128. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string and does not include or reveal the common identifier associated with the designated secured resource identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Frost or through an agent with whom Frost has contracted to receive the messages.

129. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive an access request message from the service client's application through the at least one interface, the payment request message comprising: a second service client identifier; a second transaction specific information; and a second transaction specific authentication credential whereby the second transaction specific authentication credential was received by the service client's

application from the user's application. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Frost card account holder's mobile device. The server is either hosted directly by Frost or through an agent with whom Frost has contracted to receive the messages.

130. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the user's request to access the secured resource associated with the designated secured resource identifier without transmitting or otherwise providing the common identifier of the secured resource to the service client by determining if: the first service client identifier matches the second service client identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Frost or through an agent with whom Frost has contracted to provide the authentication services.

131. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

132. Defendants thus infringe one or more claims of the 454 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 8 of the 454 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 454 Patent.

133. Frost has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

134. Frost has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 454 Patent by others and Frost will continue to do so unless enjoined by this Court. Frost's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused

Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 454 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Frost knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 454 Patent.

135. Frost continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 454 Patent.

136. Frost has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 454 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

137. Frost has committed these acts of infringement without license or authorization.

138. By engaging in the conduct described herein, Frost has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Frost is thus liable to Textile for infringement of the 454 Patent, pursuant to 35 U.S.C. § 271.

139. As a direct and proximate result of Frost's infringement of the 454 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Frost's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

140. In addition, the infringing acts and practices of Frost have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Frost is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Frost is finally and permanently enjoined from further infringement.

141. Frost has had actual knowledge of the 454 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Frost will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 454 Patent.

142. Frost has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 454 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

143. Textile has been damaged as a result of the infringing conduct by Frost alleged above. Thus, Frost is liable to Textile in an amount that adequately compensates it for such

infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

144. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 454 Patent.

ADDITIONAL ALLEGATIONS REGARDING INFRINGEMENT

145. Frost has also indirectly infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by inducing others to directly infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Frost has induced the end-users, Frost's customers, to directly infringe (literally and/or under the doctrine of equivalents) the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by using the Accused Instrumentality.

146. Frost took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

147. Such steps by Frost included, among other things, advising or directing customers and end-users to use the Accused Instrumentality in an infringing manner; advertising and promoting the use of the Accused Instrumentality in an infringing manner; and/or distributing instructions that guide users to use the Accused Instrumentality in an infringing manner.

148. Frost has performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent

and with the knowledge that the induced acts constitute infringement, at least since the filing of the Complaint.

149. Frost was and is aware that the normal and customary use of the Accused Instrumentality by Frost's customers would infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Frost's inducement is ongoing.

150. Frost directs or controls the use of the Accused Instrumentality nationwide through its own websites and in its own branches, including in Texas and elsewhere in the United States, and expects and intends that the Accused Instrumentality will be so used.

151. Frost took active steps, directly and/or through contractual relationships with others, with the specific intent to cause such persons to make or use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

152. Frost performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts would constitute infringement.

153. Frost's inducement is ongoing.

154. Frost has also indirectly infringed by contributing to the infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Frost has contributed to the direct infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by the end-user of the Accused Instrumentality.

155. The Accused Instrumentality has special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the 079

Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

156. As described above, the special features include securely authorizing specific transactions without providing a credit or debit card number to the merchant used in a manner that infringes the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

157. The special features constitute a material part of the invention of one or more of the claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and are not staple articles of commerce suitable for substantial non-infringing use.

158. Frost's contributory infringement is ongoing.

159. Frost's actions are at least objectively reckless as to the risk of infringing valid patents and this objective risk was either known or should have been known by Frost, at least since the filing of the Complaint.

160. Frost has had knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent at least since the filing of the Complaint.

161. Frost's customers have infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

162. Frost encouraged its customers' infringement.

163. Frost's direct and indirect infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent is, has been, and/or continues to be willful, intentional, deliberate, and/or in conscious disregard of Textile's rights under the patents.

164. Textile has been damaged as a result of the infringing conduct by Frost alleged above. Thus, Frost is liable to Textile in an amount that adequately compensates it for such

infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Textile hereby requests a trial by jury on all issues so triable by right.

PRAYER FOR RELIEF

Textile requests that the Court find in its favor and against Frost, and that the Court grant Textile the following relief:

- a. Judgment that one or more claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent have been infringed, either literally and/or under the doctrine of equivalents, by Frost and/or all others acting in concert therewith;
- b. A permanent injunction enjoining Frost and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert therewith from infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent; or, in the alternative, an award of a reasonable ongoing royalty for future infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by such entities;
- c. Judgment that Frost account for and pay to Textile all damages to and costs incurred by Textile because of Frost's infringing activities and other conduct complained of herein, including an award of all increased damages to which Textile is entitled under 35 U.S.C. § 284;
- d. That Textile be granted pre-judgment and post-judgment interest on the damages caused by Frost's infringing activities and other conduct complained of herein;
- e. That this Court declare this an exceptional case and award Textile its reasonable

attorney's fees and costs in accordance with 35 U.S.C. § 285; and

f. That Textile be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: October 12, 2021

Respectfully submitted,

/s/ Matthew J. Antonelli

Matthew J. Antonelli

Texas Bar No. 24068432

matt@ahtlawfirm.com

Zachariah S. Harrington

Texas Bar No. 24057886

zac@ahtlawfirm.com

Larry D. Thompson, Jr.

Texas Bar No. 24051428

larry@ahtlawfirm.com

Christopher Ryan Pinckney

Texas Bar No. 24067819

ryan@ahtlawfirm.com

ANTONELLI, HARRINGTON

& THOMPSON LLP

4306 Yoakum Blvd., Ste. 450

Houston, TX 77006

(713) 581-3000

Stafford Davis

State Bar No. 24054605

sdavis@stafforddavisfirm.com

Catherine Bartles

Texas Bar No. 24104849

cbartles@stafforddavisfirm.com

THE STAFFORD DAVIS FIRM

815 South Broadway Avenue

Tyler, Texas 75701

(903) 593-7000

(903) 705-7369 fax

Of Counsel:

Sandeep Seth

Texas State Bar No. 18043000

SETHLAW

Pennzoil Place

700 Milam Street, Suite 1300

Houston, Texas 77002
Telephone: (713) 244-5017
ss@sethlaw.com

Attorneys for Textile Computer Systems, Inc.

EXHIBIT 2E

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

TEXTILE COMPUTER SYSTEMS, INC.,

Plaintiff,

v.

INDEPENDENT BANK,

Defendant.

CIVIL ACTION NO. 6:21-cv-1054

ORIGINAL COMPLAINT FOR
PATENT INFRINGEMENT

JURY TRIAL DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Textile Computer Systems, Inc. (“Textile” or “Plaintiff”) files this original complaint against Defendant Independent Bank (“Independent Bank”), alleging, based on its own knowledge as to itself and its own actions and based on information and belief as to all other matters, as follows:

PARTIES

1. Textile Computer Systems, Inc. is a corporation formed under the laws of the State of Texas, with a place of business at 618 Bluff Trail, San Antonio, Texas, 78216.
2. Independent Bank is a bank duly organized and existing under the laws of Texas. Independent Bank has places of business in Waco, Texas and Austin, Texas.
3. Independent Bank and its affiliates lead and are part of an interrelated group of companies which together comprise one of the country’s largest banking and financial service entities, including under the Independent Bank brand.
4. Independent Bank and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

5. Independent Bank and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

6. Independent Bank and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

7. Thus, Independent Bank and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

JURISDICTION AND VENUE

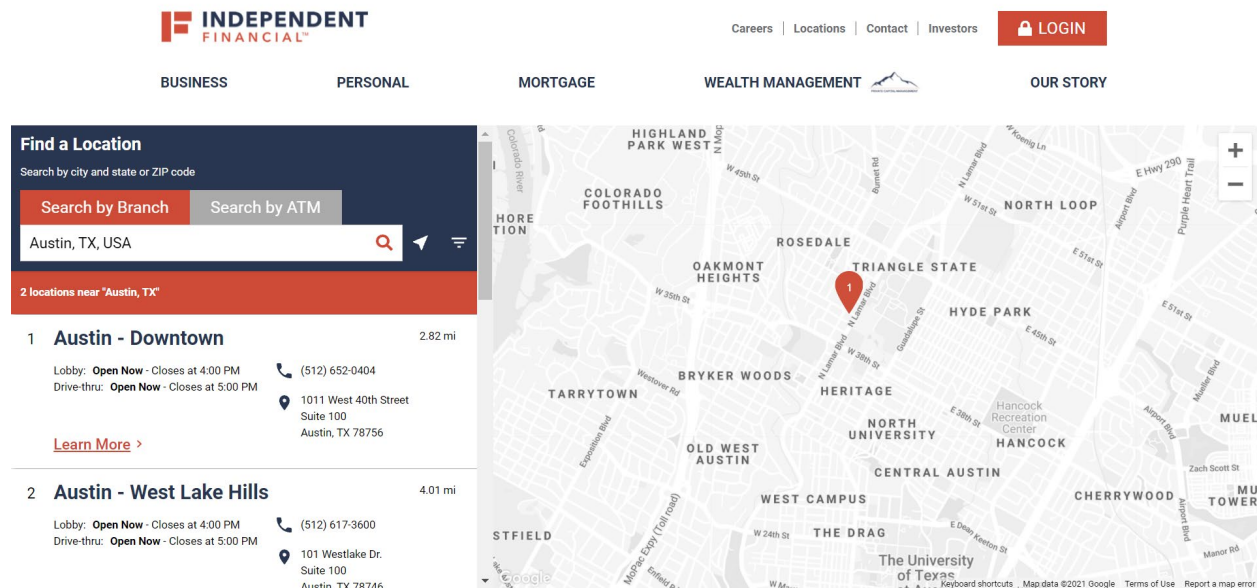
8. This is an action for infringement of United States patents arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. § 1331 and § 1338(a).

9. This Court has personal jurisdiction over Independent Bank pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Independent Bank has done and continues to do business in Texas; and (ii) Independent Bank has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations, inducing others to commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein.

10. Venue is proper in this district pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Independent Bank has committed and continues to commit acts of patent infringement in this district. For example, Independent Bank cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment

systems, those cardholders make and/or use the accused instrumentalities in the district.

Independent Bank induces others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. Independent Bank has regular and established places of business in this district, including at least at 8004 Woodway Drive, Suite 200, Waco, Texas 76712, at 1011 W. 40th Street, Suite 100, Austin, Texas 78756, and at numerous other locations in Waco and Austin:



(Source: <https://locations.ifinancial.com/search?q=30.267153%2C-97.7430608&type=location&qp=Austin%2C%20TX%2C%20USA&r=10&l=en>)



(Source: screenshot from Google Maps Street View)

[Careers](#) | [Locations](#) | [Contact](#) | [Investors](#)

LOGIN

[BUSINESS](#)
[PERSONAL](#)
[MORTGAGE](#)
[WEALTH MANAGEMENT](#)
[OUR STORY](#)

Find a Location

Search by city and state or ZIP code

Search by Branch

Search by ATM

2 locations near "Waco, TX"

- Waco - Bosque** 2.97 mi

Lobby: **Open Now** - Closes at 4:00 PM
 Drive-thru: **Open Now** - Closes at 6:00 PM

(254) 399-6366
 5401 Bosque Blvd.
 Waco, TX 76710

[Learn More >](#)
- Waco - Woodway** 5.49 mi

Lobby: **Open Now** - Closes at 4:00 PM
 Drive-thru: **Open Now** - Closes at 6:00 PM

(254) 741-6121
 8004 Woodway Drive
 Suite 200
 Waco, TX 76712

[Learn More >](#)

(Source: <https://locations.ifinancial.com/search?q=31.549333%2C-97.1466695&type=location&qp=Waco%2C%20TX%2C%20USA&r=10&l=en>)



(Source: screenshot from Google Maps Street View)

BACKGROUND

11. The patents-in-suit generally pertain to payment authorization technology used in payment networks used to process transactions from, for example, credit cards and debit cards. The technology disclosed by the patents was developed by Gopal Nandakumar, a Texas-based entrepreneur, software engineer, and prolific inventor with over 30 years of experience in the field of Information Management Systems.

12. In 1987, after receiving Master's Degrees from both the University of Madras, India and the Georgia Institute of Technology, Mr. Nandakumar formed Textile Computer Systems, Inc. ("Textile") for the purpose of consulting and developing software for the textile industry. In 2005, Textile began transitioning into credit card transaction systems. In 2011, Textile began to develop and market the MySingleLink suite of applications.

13. The Nandakumar patents are related to payment authorization technology. Mr. Nandakumar has been at the forefront of payment authorization, developing, disclosing, and patenting solutions for reducing fraud in credit and debit card transactions. Indeed, the

Nandakumar patents (or the applications leading to them) have been cited during patent prosecution over a hundred times, including by numerous leading companies in the payment authorization industry such as ADP, Bank of America, Google, Groupon, IBM, Mastercard, NEC, Paypal, Visa, and Wells Fargo.

THE TECHNOLOGY

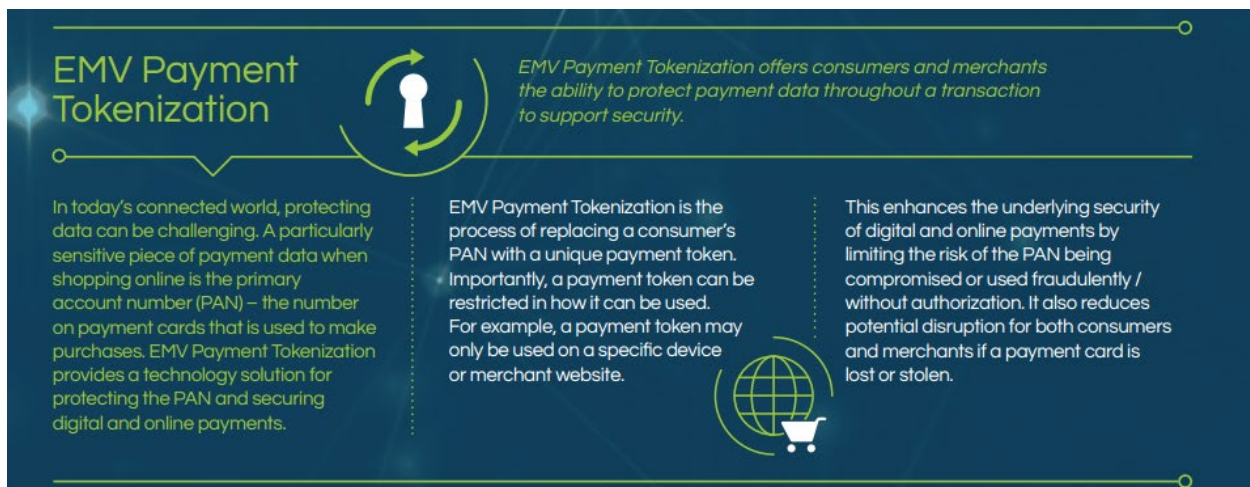
14. The patents-in-suit, U.S. Patent Nos. 8,505,079, 8,533,802, 9,584,499, 10,148,659, and 10,560,454 (collectively, the “Asserted Patents”), teach systems, including payment processing systems, for securely and effectively approving and processing specific credit card and/or debit card transactions. Through the specific use of servers, messaging gateways, and/or interfaces, these systems act to reduce credit card and/or debit card fraud and misuse through their use and validation of key strings, authentication credentials, transaction specific information, and transaction specific credentials. The technology in the Asserted Patents improves the underlying functionality of existing card processing infrastructure by minimizing fraud and data theft in the face of attacks on payment systems that continue to grow in their number and sophistication.

15. The patented improvements are critical for implementing secure payment systems, especially in light of the many high-profile merchant data breaches that have led to increased credit and debit card fraud. For example, in 2006, TJX Companies, who owns retailers like TJMaxx and Marshall’s, was hit with a cyber attack that resulted in the theft of credit cards leading to over \$100 million in fraud losses. In 2013, five people were indicted for attacking a number of retailers and financial institutions including NASDAQ, 7-Eleven, JCP, and others, stealing over 160 million cards. Also in 2013, the retailer Target suffered a data breach that resulted in 40 million debit and credit cards being compromised.

16. One implementation of the technology claimed in the Asserted Patents has been described by EMVCo as “a global Payment Tokenisation ecosystem that overlays and interoperates with existing payment ecosystems to support digital commerce and new methods of payment” and as “enhanc[ing] the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorized or fraudulent use of PANs.” (Source: <https://www.emvco.com/emv-technologies/payment-tokenisation/>).

17. The technology claimed in the Asserted Patents is far from conventional technology. The payment industry gathered and consulted experts who worked together over a number of years to develop infringing payment tokenisation systems. In other words, the technology claimed in the Asserted Patents was not existing or conventional technology that the payment industry had sitting on the shelf.

18. Indeed, as recently as February of this year, EMVCo itself recognized that an implementation of the technology claimed in the Asserted Patents “provides a technology solution for protecting the PAN and securing digital and online payments”:



(Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

19. That same EMVCo document notes that “In today’s connected world, protecting data can be challenging. A particularly sensitive piece of payment data when shopping online is the primary account number (PAN) – the number on payment cards that is used to make purchases” and that EMVCo’s payment tokenization “enhances the underlying security of digital and online payments by limiting the risk of the PAN being compromised or used fraudulently / without authorization.” The document also states that the “Payment Tokenisation Specification provides an interoperable Technical Framework.” (Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

20. One of the asserted patents, the 079 Patent, was challenged in an Inter Partes Review proceeding before the Patent and Trademark Office (“PTO”). The PTO found that the challenger, Unified Patents Inc., was unable to show that one element, the “key string” as claimed in the 079 Patent claims and as construed by the PTO, was in the prior art at all, much less it being conventional or widespread. The PTO thus confirmed the patentability of all challenged claims of the 079 Patent.

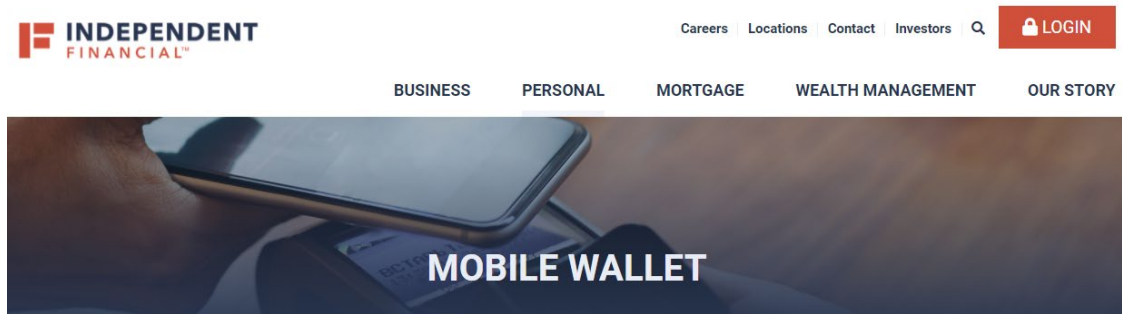
COUNT I

INFRINGEMENT OF U.S. PATENT NO. 8,505,079

21. On August 6, 2013, United States Patent No. 8,505,079 (“the 079 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

22. Textile is the owner of the 079 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 079 Patent against infringers, and to collect damages for all relevant times.

23. Independent Bank offers debit and/or credit cards, such as the Independent Bank Visa Platinum Card, that are used with an authentication system that authenticates the identity of an Independent Bank card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Independent Bank card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities, for example. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.



MORE WAYS TO PAY IN MORE PLACES THAN EVER. USE YOUR SMARTPHONE TO MAKE IN-STORE OR IN-APP PURCHASES.

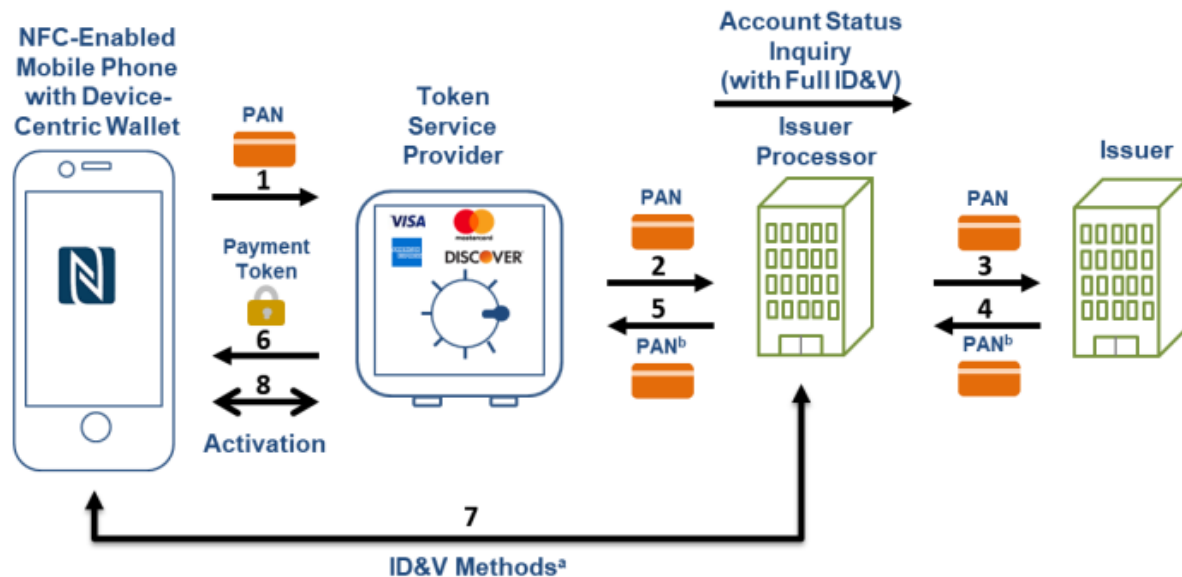
Details

- Available through Apple Pay®, Google Pay™, or Samsung Pay®
- Make purchases quickly and securely with your mobile device
- Pay in an easier way — no more counting change or carrying cards
- Easily set up payment information
- Add multiple cards to your device for extra convenience
- Keep purchases private — card data is never directly transmitted to retailers
- Easily protect your accounts if you lose your device

(Source: <https://www.independent-bank.com/personal/account-services/mobile-wallet.html>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^a ID&V methods includes text or email or call. OTP is an example.

^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

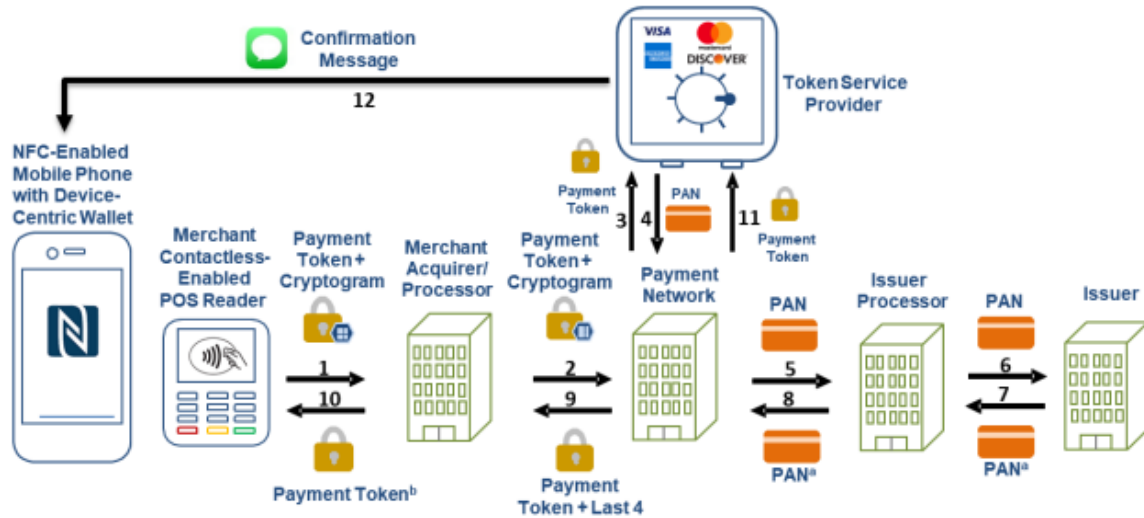
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

24. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, an Independent Bank account holder requests Independent Bank to provision a specific Independent Bank debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Independent Bank card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating

the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

25. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Independent Bank card account holders for provisioning a specific Independent Bank debit and/or credit card for use on their mobile devices. The messaging gateway is also programmed to receive requests initiated by Independent Bank card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Independent Bank card account of the account holder. This messaging gateway is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to receive the messages.

26. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to determine a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for

authenticating the identity of said requester. For example, behind the firewall of the messaging gateway and in secure communication therewith is an authorization server that processes the received request to identify the token value sent for the account selected to be charged that was passed from the authorized user to the merchant terminal via the NFC communication link. From the token value, the server can look up the debit and/or credit card account number. The authorization server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to provide the authentication services.

27. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive within the payment authorization request transaction specific information that was input into the request by the merchant. The interface is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to provide the authentication services.

28. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

29. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

30. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

31. Defendants thus infringe one or more of the claims of the 079 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 079 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 079 Patent.

32. Independent Bank has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(a), by making, using, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

33. Independent Bank has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 079 Patent by

others and Independent Bank will continue to do so unless enjoined by this Court. Independent Bank's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 079 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Independent Bank knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 079 Patent.

34. Independent Bank continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 079 Patent.

35. Independent Bank has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 079 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for

use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

36. Independent Bank has committed these acts of infringement without license or authorization.

37. By engaging in the conduct described herein, Independent Bank has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Independent Bank is thus liable to Textile for infringement of the 079 Patent, pursuant to 35 U.S.C. § 271.

38. As a direct and proximate result of Independent Bank's infringement of the 079 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Independent Bank's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

39. In addition, the infringing acts and practices of Independent Bank have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Independent Bank is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Independent Bank is finally and permanently enjoined from further infringement.

40. Independent Bank has had actual knowledge of the 079 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Independent Bank will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 079 Patent.

41. Independent Bank has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 079 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

42. Textile has been damaged as a result of the infringing conduct by Independent Bank alleged above. Thus, Independent Bank is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

43. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 079 Patent.

COUNT II

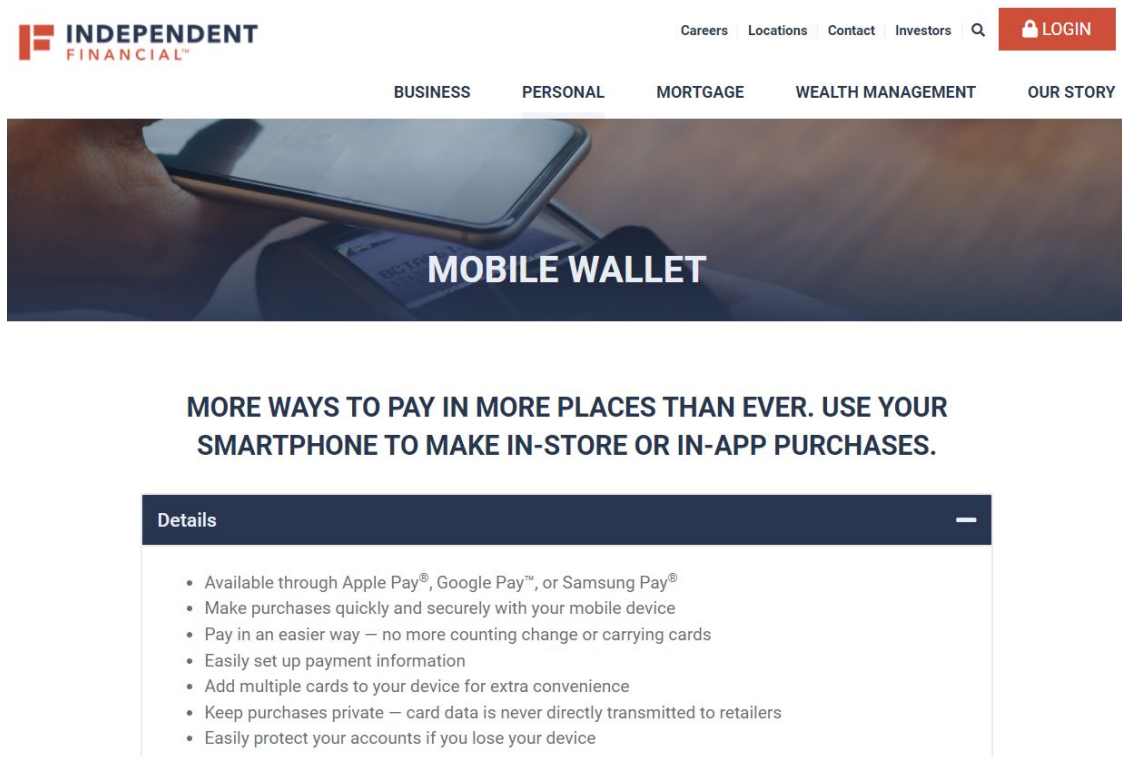
INFRINGEMENT OF U.S. PATENT NO. 8,533,802

44. On September 10, 2013, United States Patent No. 8,533,802 (“the 802 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

45. Textile is the owner of the 802 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 802 Patent against infringers, and to collect damages for all relevant times.

46. Independent Bank offers debit and/or credit cards, such as the Independent Bank Visa Platinum Card, that are used with an authentication system that authenticates the identity of an Independent Bank card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Independent Bank card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise

provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



The screenshot shows the Independent Financial website. The header includes the logo, navigation links (Careers, Locations, Contact, Investors, Q), and a LOGIN button. The main navigation bar lists BUSINESS, PERSONAL, MORTGAGE, WEALTH MANAGEMENT, and OUR STORY. Below this is a large banner image of a hand holding a smartphone over a payment terminal, with the text "MOBILE WALLET" overlaid. Underneath the banner is a heading: "MORE WAYS TO PAY IN MORE PLACES THAN EVER. USE YOUR SMARTPHONE TO MAKE IN-STORE OR IN-APP PURCHASES." Below the heading is a "Details" section with a list of bullet points.

INDEPENDENT FINANCIAL

Careers | Locations | Contact | Investors | Q | LOGIN

BUSINESS | PERSONAL | MORTGAGE | WEALTH MANAGEMENT | OUR STORY

MOBILE WALLET

MORE WAYS TO PAY IN MORE PLACES THAN EVER. USE YOUR SMARTPHONE TO MAKE IN-STORE OR IN-APP PURCHASES.

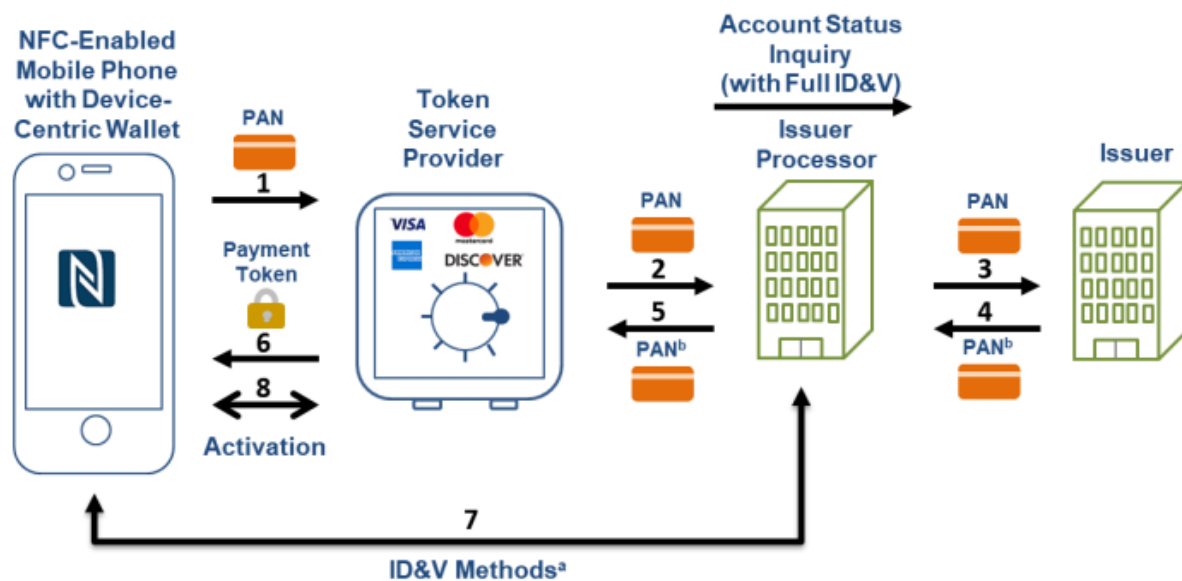
Details

- Available through Apple Pay®, Google Pay™, or Samsung Pay®
- Make purchases quickly and securely with your mobile device
- Pay in an easier way — no more counting change or carrying cards
- Easily set up payment information
- Add multiple cards to your device for extra convenience
- Keep purchases private — card data is never directly transmitted to retailers
- Easily protect your accounts if you lose your device

(Source: <https://www.independent-bank.com/personal/account-services/mobile-wallet.html>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

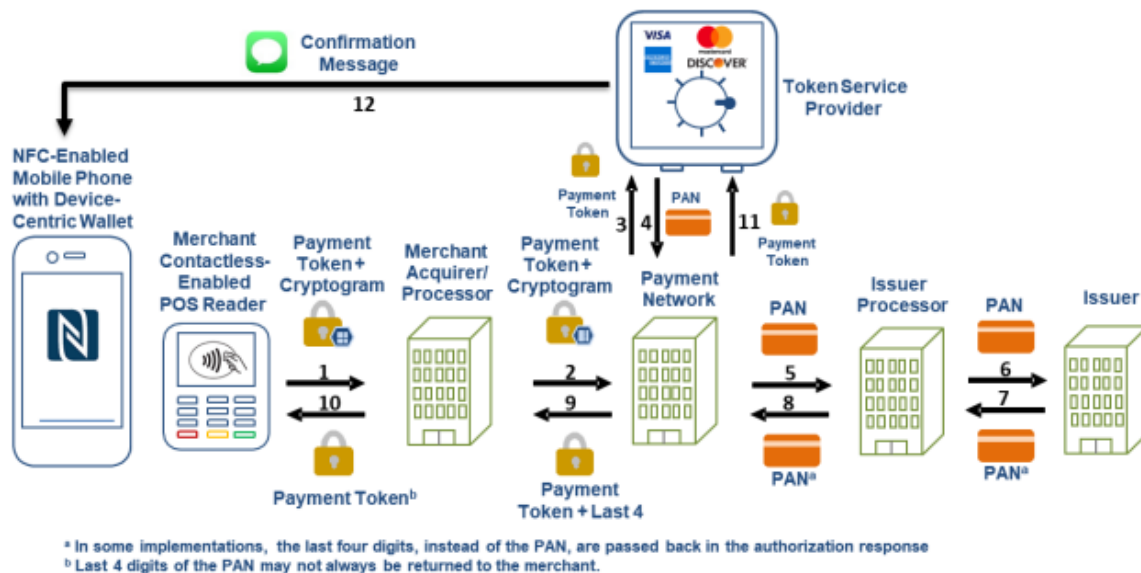


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

47. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, an Independent Bank account holder requests Independent Bank to provision a specific Independent Bank debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Independent Bank card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating

the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

48. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Independent Bank card account holders for provisioning a specific Independent Bank debit and/or credit card for use on their mobile devices. This messaging gateway is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to receive the messages.

49. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate a key string adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the message gateway and in secure communication therewith is an authorization server that generates a token corresponding to the debit and/or credit card account number. The authorization server is either hosted directly

by Independent Bank or through an agent with whom Independent Bank has contracted to provide the authentication services.

50. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive transaction specific information that was input into the request by the merchant, *e.g.*, the merchant ID, invoice number, invoice amount, and date/timestamp. The interface is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to provide the authentication services.

51. The Accused Instrumentality includes a first set of instructions further operable to communicate the key string to the authorized user that the requester purports to be. For example, the messaging gateway sends the generated token to the authorized user's mobile device for use in merchant transactions.

52. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

53. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For

example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

54. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

55. Defendants thus infringe one or more claims of the 802 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 802 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 802 Patents.

56. Independent Bank has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

57. Independent Bank has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 802 Patent by others and Independent Bank will continue to do so unless enjoined by this Court. Independent

Bank's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 802 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Independent Bank knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 802 Patent.

58. Independent Bank continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 802 Patent.

59. Independent Bank has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 802 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for

use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

60. Independent Bank has committed these acts of infringement without license or authorization.

61. By engaging in the conduct described herein, Independent Bank has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Independent Bank is thus liable to Textile for infringement of the 802 Patent, pursuant to 35 U.S.C. § 271.

62. As a direct and proximate result of Independent Bank's infringement of the 802 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Independent Bank's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

63. In addition, the infringing acts and practices of Independent Bank have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Independent Bank is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Independent Bank is finally and permanently enjoined from further infringement.

64. Independent Bank has had actual knowledge of the 802 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Independent Bank will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 802 Patent.

65. Independent Bank has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 802 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

66. Textile has been damaged as a result of the infringing conduct by Independent Bank alleged above. Thus, Independent Bank is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

67. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 802 Patent.

COUNT III

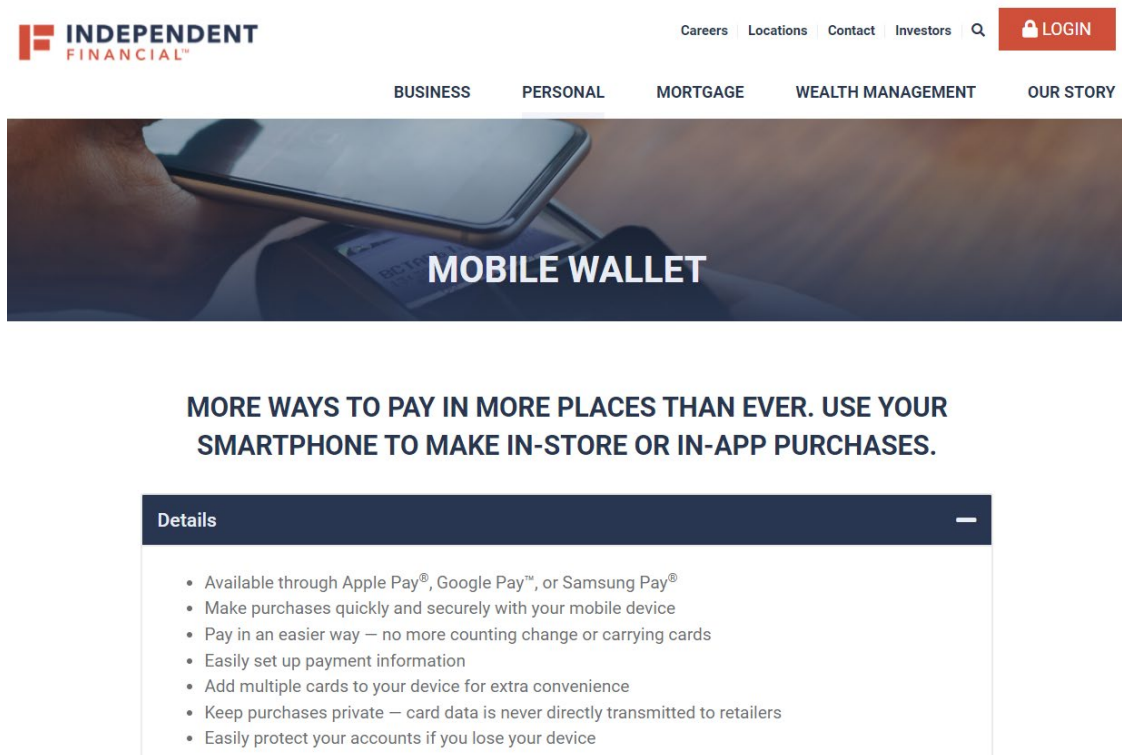
INFRINGEMENT OF U.S. PATENT NO. 9,584,499

68. On February 28, 2017, United States Patent No. 9,584,499 (“the 499 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

69. Textile is the owner of the 499 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 499 Patent against infringers, and to collect damages for all relevant times.

70. Independent Bank offers debit and/or credit cards, such as the Independent Bank Visa Platinum Card, that are used by Independent Bank in practicing a method for authorizing transaction specific access to a secured resource having a secured resource identity (the “Accused Instrumentality”). The Independent Bank transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card

number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



The screenshot shows the Independent Financial website. The header includes the logo, navigation links (Careers, Locations, Contact, Investors, LOGIN), and a search icon. Below the header is a navigation bar with links for BUSINESS, PERSONAL, MORTGAGE, WEALTH MANAGEMENT, and OUR STORY. The main content area features a large image of a smartphone being used to make a payment, with the text "MOBILE WALLET" overlaid. Below this is a section titled "MORE WAYS TO PAY IN MORE PLACES THAN EVER. USE YOUR SMARTPHONE TO MAKE IN-STORE OR IN-APP PURCHASES." followed by a "Details" section containing a bulleted list of features.

INDEPENDENT FINANCIAL™

Careers | Locations | Contact | Investors | **LOGIN**

BUSINESS | PERSONAL | MORTGAGE | WEALTH MANAGEMENT | OUR STORY

MOBILE WALLET

MORE WAYS TO PAY IN MORE PLACES THAN EVER. USE YOUR SMARTPHONE TO MAKE IN-STORE OR IN-APP PURCHASES.

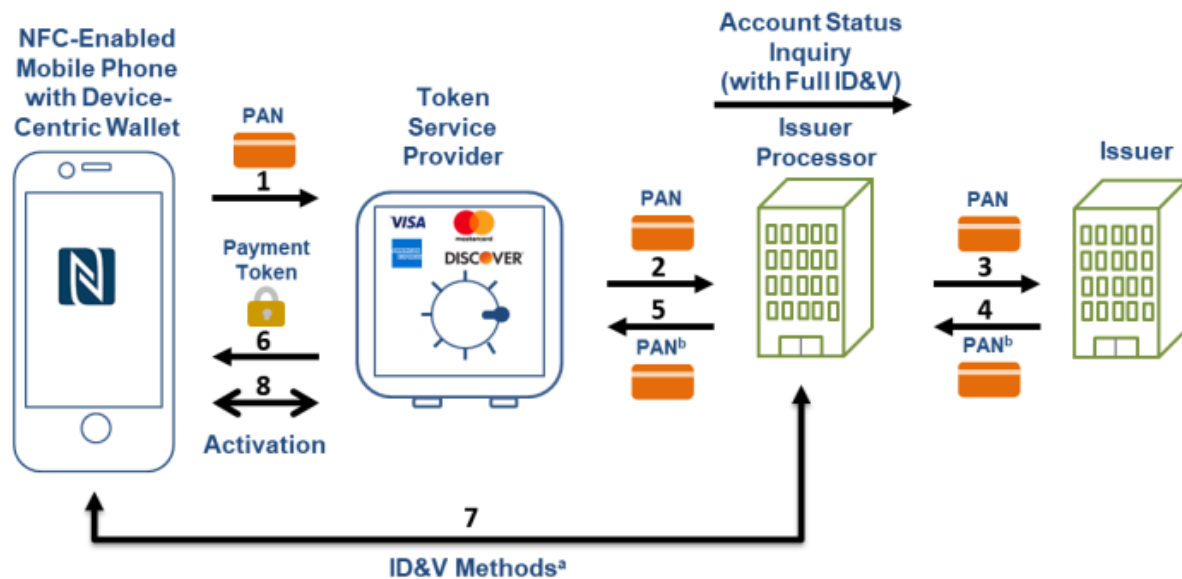
Details

- Available through Apple Pay®, Google Pay™, or Samsung Pay®
- Make purchases quickly and securely with your mobile device
- Pay in an easier way — no more counting change or carrying cards
- Easily set up payment information
- Add multiple cards to your device for extra convenience
- Keep purchases private — card data is never directly transmitted to retailers
- Easily protect your accounts if you lose your device

(Source: <https://www.independent-bank.com/personal/account-services/mobile-wallet.html>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

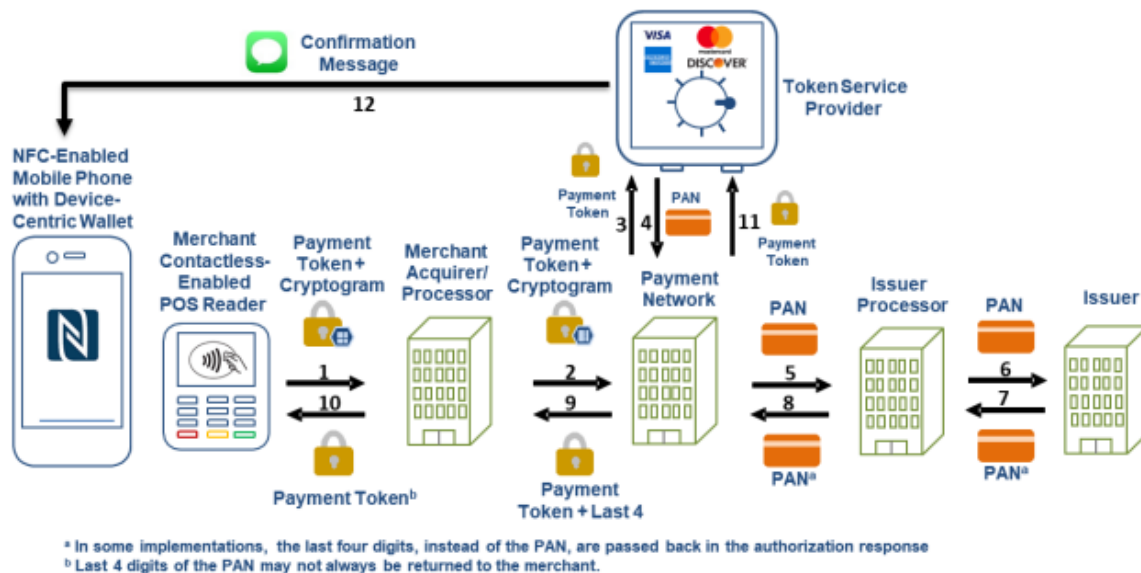


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

71. Independent Bank's use of the Accused Instrumentality includes a method for authorizing transaction specific access to a secured resource having a secured resource identity. For example, an Independent Bank account holder requests Independent Bank to provision a specific Independent Bank debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Independent Bank card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter.

In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram.

72. The Accused Instrumentality includes receiving at a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive a request for transaction specific access to a secured resource by a service client. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Independent Bank card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Independent Bank card account of the account holder. This messaging gateway is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to receive the messages.

73. The Accused Instrumentality includes generating a key string with a server in communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate the key string known to both said server and an authorized user of the secured resource, said key string being associated with the secured resource within a key string table accessible by the server and providing a basis for authenticating the secured resource identity by searching the key string table for the key string. For example, behind the firewall of the messaging gateway and in communication therewith is

an authorization server that generates a token corresponding to a secured resource during the provisioning process. After this, the authorization server updates a table that maps token numbers to secured resource identities. The authorization server is then able to search the table to authenticate a secured resource identity by searching the table for the token. If the token has a corresponding secured resource identity, that identity is authenticated. The authorization server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to provide the authentication services.

74. The Accused Instrumentality includes determining transaction specific information with the server in communication with the messaging gateway, the server having a third set of instructions embodied in a computer readable medium operable to identify transaction specific information within the request. For example, the authorization server is also programmed to identify within the payment authorization request transaction specific information that was passed by the merchant. The authorization server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to provide the authentication services.

75. The Accused Instrumentality includes communicating said key string to said authorized user. For example, once the provisioning process is complete, the messaging gateway and/or the server send the token to the authorized user's mobile device. The messaging gateway is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to provide the authentication services. The authorization server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to provide the authentication services.

76. The Accused Instrumentality includes receiving an authentication credential from said service client, said authentication credential having been provided to said service client by said authorized user. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant. The authorization server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to provide the authentication services.

77. The Accused Instrumentality includes evaluating said authentication credential. For example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authorizes the transaction specific access. The authorization server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to provide the authentication services.

78. The Accused Instrumentality includes wherein the key string and authentication credential do not reveal any primary identifier associated with said secured resource. For example, neither the token nor the cryptogram reveals the debit and/or credit card number associated with the secured resource.

79. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

80. Defendants thus infringe one or more claims of the 499 Patent. The elements and conduct described herein are covered by and infringe upon at least Claim 3 of the 499 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 499 Patent.

81. Independent Bank has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

82. Independent Bank has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 499 Patent by others and Independent Bank will continue to do so unless enjoined by this Court. Independent Bank's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 499 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Independent Bank knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 499 Patent.

83. Independent Bank continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 499 Patent.

84. Independent Bank has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 499 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

85. Independent Bank has committed these acts of infringement without license or authorization.

86. By engaging in the conduct described herein, Independent Bank has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Independent Bank is thus liable to Textile for infringement of the 499 Patent, pursuant to 35 U.S.C. § 271.

87. As a direct and proximate result of Independent Bank's infringement of the 499 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an

amount adequate to compensate Textile for Independent Bank's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

88. In addition, the infringing acts and practices of Independent Bank have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Independent Bank is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Independent Bank is finally and permanently enjoined from further infringement.

89. Independent Bank has had actual knowledge of the 499 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Independent Bank will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 499 Patent.

90. Independent Bank has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 499 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

91. Textile has been damaged as a result of the infringing conduct by Independent Bank alleged above. Thus, Independent Bank is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

92. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 499 Patent.


COUNT IV


INFRINGEMENT OF U.S. PATENT NO. 10,148,659


93. On December 4, 2018, United States Patent No. 10,148,659 (“the 659 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

94. Textile is the owner of the 659 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 659 Patent against infringers, and to collect damages for all relevant times.


95. Independent Bank offers debit and/or credit cards, such as the Independent Bank Visa Platinum Card, that are used with a computer-implemented system for a credit or debit and/or credit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit and/or credit card account number to the merchant (the “Accused Instrumentality”). The Independent Bank transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.



Careers | Locations | Contact | Investors | 

 LOGIN

BUSINESSPERSONALMORTGAGEWEALTH MANAGEMENTOUR STORY



MOBILE WALLET

MORE WAYS TO PAY IN MORE PLACES THAN EVER. USE YOUR SMARTPHONE TO MAKE IN-STORE OR IN-APP PURCHASES.

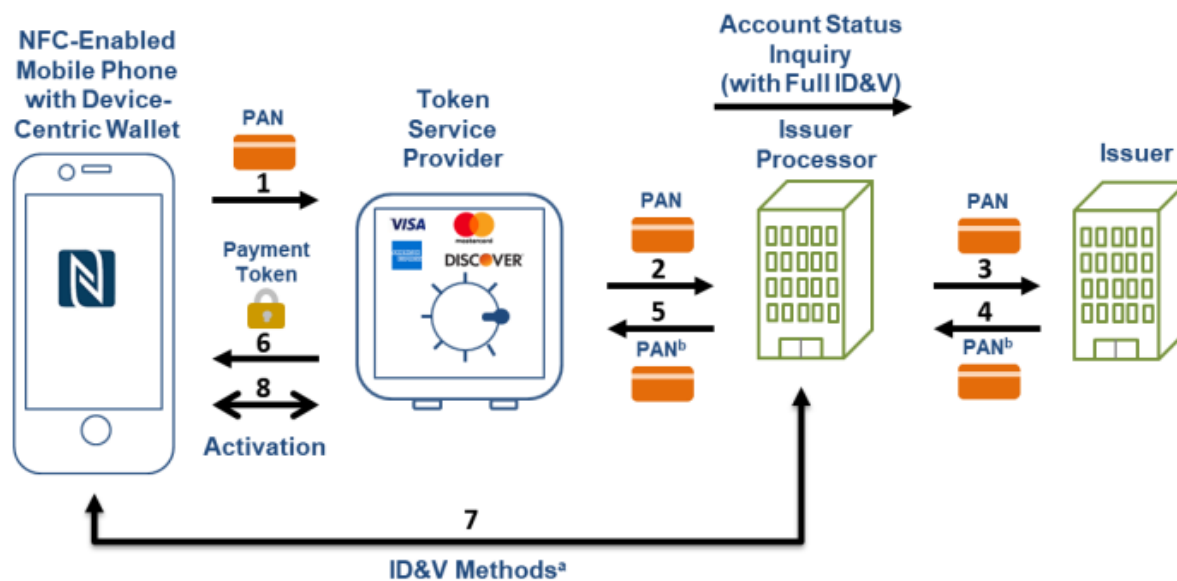
Details

- Available through Apple Pay®, Google Pay™, or Samsung Pay®
- Make purchases quickly and securely with your mobile device
- Pay in an easier way — no more counting change or carrying cards
- Easily set up payment information
- Add multiple cards to your device for extra convenience
- Keep purchases private — card data is never directly transmitted to retailers
- Easily protect your accounts if you lose your device

(Source: <https://www.independent-bank.com/personal/account-services/mobile-wallet.html>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

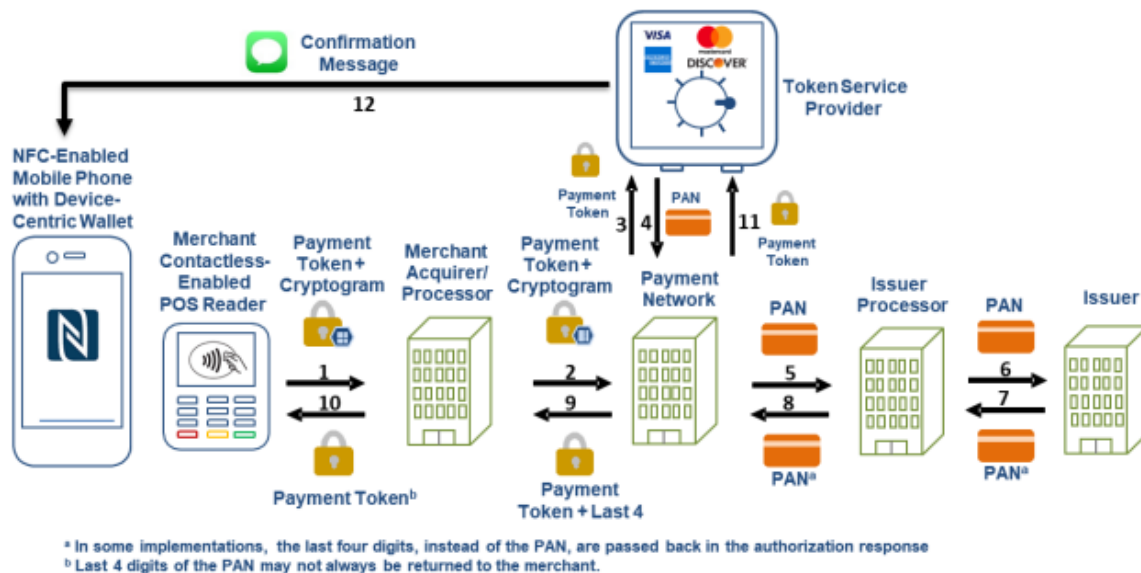


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

96. The Accused Instrumentality includes a computer-implemented system for a credit or debit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit card account number to the merchant. For example, an Independent Bank account holder requests Independent Bank to provision a specific Independent Bank debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Independent Bank to a specific merchant in a specific amount for a

specific transaction from a specific Independent Bank card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

97. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a credit or debit card account holder's mobile device, a merchant's payment application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with an Independent Bank card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Independent Bank card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Independent Bank card account of the account holder. This interface is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to receive the messages.

98. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration

information received from the credit or debit card account holder through the at least one interface, the registration information comprising a credit or debit card account holder identifier and at least one credit or debit card account number having an associated unique account identifier wherein the credit or debit card account number and unique account identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card and the debit and/or credit card account number (which has a corresponding token), received from Independent Bank card account holders through the interface for provisioning a specific Independent Bank debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Independent Bank card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Independent Bank card account of the account holder. The server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to receive the messages.

99. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to pay the specific merchant for the specific transaction from a given debit or credit card account, the authorization request message having been received through the at least one interface and originating from the credit or debit card account holder's mobile device and comprising: a first merchant identifier; a first transaction specific information selected from the group consisting of a first transaction amount and first client reference identifier; the credit or debit card account holder identifier; and a designated unique account

identifier selected from the at least one unique account identifiers. For example, the Accused Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Independent Bank card account holder's mobile device. The server is programmed to receive authorization requests initiated by Independent Bank card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a merchant identifier, and the Independent Bank card account holder identifier. The server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to receive the messages.

100. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string wherein the key string is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the designated unique account identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to receive the messages.

101. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive a payment request message from the merchant's payment application through the at least one interface, the payment request message comprising: a second merchant identifier; a second transaction specific information selected from the group consisting of a second transaction amount and second client reference identifier; and a second transaction specific authentication credential whereby the second authentication credential was received by the merchant application from the credit or debit card account holder's mobile device. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Independent Bank card account holder's mobile device. The server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to receive the messages.

102. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the credit or debit card account holder's request to use the credit or debit card account number associated with the designated unique account identifier for payment to the specific merchant for the specific transaction and authorizing the resource provider to use the credit or debit card account number associated with the designated unique account identifier to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or bank account number to the

specific merchant by determining if: the first merchant identifier matches the second merchant identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to provide the authentication services.

103. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

104. Defendants thus infringe one or more claims of the 659 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 9 of the 659 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 659 Patent.

105. Independent Bank has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

106. Independent Bank has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 659 Patent by others and Independent Bank will continue to do so unless enjoined by this Court. Independent Bank's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 659 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Independent Bank knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 659 Patent.

107. Independent Bank continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 659 Patent.

108. Independent Bank has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 659 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

109. Independent Bank has committed these acts of infringement without license or authorization.

110. By engaging in the conduct described herein, Independent Bank has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Independent Bank is thus liable to Textile for infringement of the 659 Patent, pursuant to 35 U.S.C. § 271.

111. As a direct and proximate result of Independent Bank's infringement of the 659 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Independent Bank's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

112. In addition, the infringing acts and practices of Independent Bank have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at

law, and for which Independent Bank is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Independent Bank is finally and permanently enjoined from further infringement.

113. Independent Bank has had actual knowledge of the 659 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Independent Bank will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 659 Patent.

114. Independent Bank has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 659 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

115. Textile has been damaged as a result of the infringing conduct by Independent Bank alleged above. Thus, Independent Bank is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

116. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 659 Patent.


COUNT V


INFRINGEMENT OF U.S. PATENT NO. 10,560,454


117. On February 11, 2020, United States Patent No. 10,560,454 (“the 454 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

118. Textile is the owner of the 454 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 454 Patent against infringers, and to collect damages for all relevant times.


119. Independent Bank offers debit and/or credit cards, such as the Independent Bank Visa Platinum Card, that are used with a computer-implemented system for a user to authorize a resource authorize a service client’s access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource’s common identifier to the service client (the “Accused Instrumentality”). The Independent Bank transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.



Careers | Locations | Contact | Investors | 

 LOGIN

BUSINESSPERSONALMORTGAGEWEALTH MANAGEMENTOUR STORY



MOBILE WALLET

MORE WAYS TO PAY IN MORE PLACES THAN EVER. USE YOUR SMARTPHONE TO MAKE IN-STORE OR IN-APP PURCHASES.

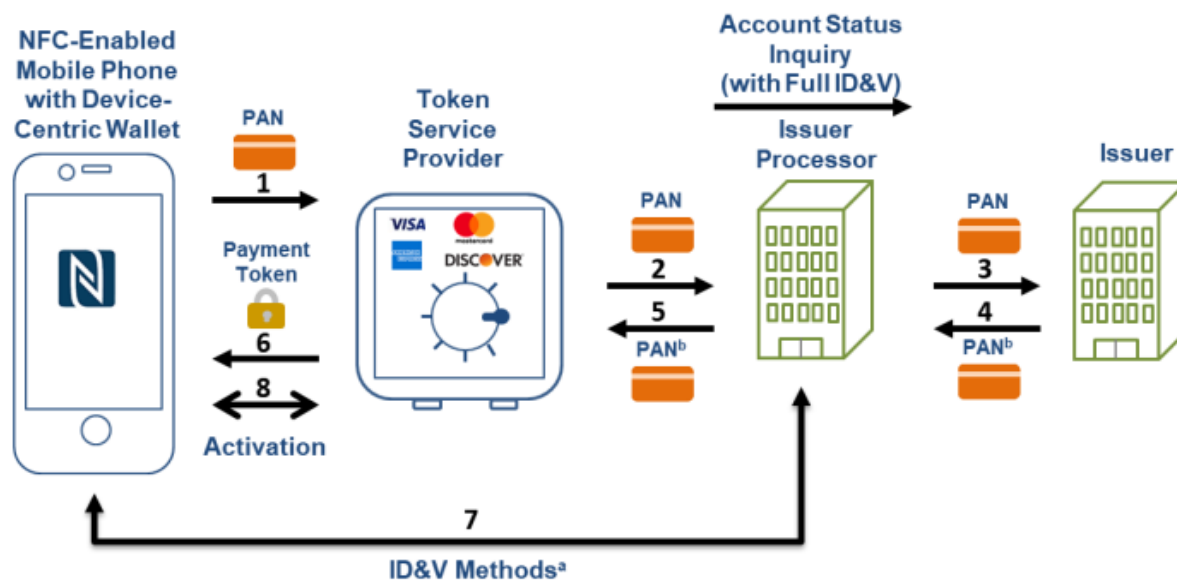
Details

- Available through Apple Pay®, Google Pay™, or Samsung Pay®
- Make purchases quickly and securely with your mobile device
- Pay in an easier way — no more counting change or carrying cards
- Easily set up payment information
- Add multiple cards to your device for extra convenience
- Keep purchases private — card data is never directly transmitted to retailers
- Easily protect your accounts if you lose your device

(Source: <https://www.independent-bank.com/personal/account-services/mobile-wallet.html>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

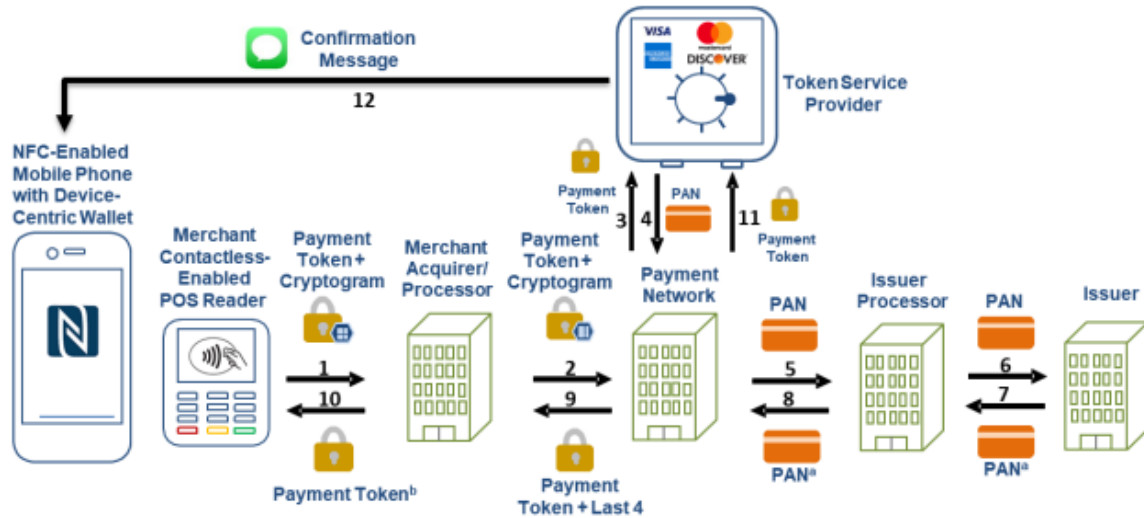
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

120. The Accused Instrumentality includes a computer-implemented system for a user to authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client. For example, an Independent Bank account holder requests Independent Bank to provision a specific Independent Bank debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Independent Bank to a specific merchant in a specific amount for a specific transaction from a specific Independent

Bank card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

121. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a user's application, a service client's application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with an Independent Bank card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Independent Bank card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Independent Bank card account of the account holder. This interface is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to receive the messages.

122. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration

information received from the user through the at least one interface, the registration information comprising a user identifier and at least one secured resource identifier associated with the common identifier of the secured resource, wherein the common identifier and secured resource identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card, the debit and/or credit card account number (which has a corresponding token), and the CVV number received from Independent Bank card account holders through the interface for provisioning a specific Independent Bank debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Independent Bank card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Independent Bank card account of the account holder. The server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to receive the messages.

123. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to authorize access to the secured resource by the service client, the authorization request message having been received through the at least one interface from the user's application and comprising: a first service client identifier; a first transaction specific information; the user identifier; and a designated secured resource identifier selected from one of the at least one secured resource identifiers. For example, the Accused Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Independent

Bank card account holder's mobile device. The server is programmed to receive authorization requests initiated by Independent Bank card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a CVV number, a merchant identifier, other token information, and the Independent Bank card account holder identifier. The server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to receive the messages.

124. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string and does not include or reveal the common identifier associated with the designated secured resource identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to receive the messages.

125. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive an access

request message from the service client's application through the at least one interface, the payment request message comprising: a second service client identifier; a second transaction specific information; and a second transaction specific authentication credential whereby the second transaction specific authentication credential was received by the service client's application from the user's application. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Independent Bank card account holder's mobile device. The server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to receive the messages.

126. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the user's request to access the secured resource associated with the designated secured resource identifier without transmitting or otherwise providing the common identifier of the secured resource to the service client by determining if: the first service client identifier matches the second service client identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment

request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Independent Bank or through an agent with whom Independent Bank has contracted to provide the authentication services.

127. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

128. Defendants thus infringe one or more claims of the 454 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 8 of the 454 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 454 Patent.

129. Independent Bank has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

130. Independent Bank has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 454 Patent by

others and Independent Bank will continue to do so unless enjoined by this Court. Independent Bank's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 454 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Independent Bank knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 454 Patent.

131. Independent Bank continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 454 Patent.

132. Independent Bank has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 454 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an

infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

133. Independent Bank has committed these acts of infringement without license or authorization.

134. By engaging in the conduct described herein, Independent Bank has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Independent Bank is thus liable to Textile for infringement of the 454 Patent, pursuant to 35 U.S.C. § 271.

135. As a direct and proximate result of Independent Bank's infringement of the 454 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Independent Bank's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

136. In addition, the infringing acts and practices of Independent Bank have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Independent Bank is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Independent Bank is finally and permanently enjoined from further infringement.

137. Independent Bank has had actual knowledge of the 454 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Independent Bank will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 454 Patent.

138. Independent Bank has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 454 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

139. Textile has been damaged as a result of the infringing conduct by Independent Bank alleged above. Thus, Independent Bank is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

140. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 454 Patent.

ADDITIONAL ALLEGATIONS REGARDING INFRINGEMENT

141. Independent Bank has also indirectly infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by inducing others to directly infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Independent Bank has induced the end-users, Independent Bank’s customers, to directly infringe (literally and/or under the doctrine of equivalents) the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by using the Accused Instrumentality.

142. Independent Bank took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

143. Such steps by Independent Bank included, among other things, advising or directing customers and end-users to use the Accused Instrumentality in an infringing manner;

advertising and promoting the use of the Accused Instrumentality in an infringing manner; and/or distributing instructions that guide users to use the Accused Instrumentality in an infringing manner.

144. Independent Bank has performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts constitute infringement, at least since the filing of the Complaint.

145. Independent Bank was and is aware that the normal and customary use of the Accused Instrumentality by Independent Bank's customers would infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Independent Bank's inducement is ongoing.

146. Independent Bank directs or controls the use of the Accused Instrumentality nationwide through its own websites and in its own branches, including in Texas and elsewhere in the United States, and expects and intends that the Accused Instrumentality will be so used.

147. Independent Bank took active steps, directly and/or through contractual relationships with others, with the specific intent to cause such persons to make or use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

148. Independent Bank performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts would constitute infringement.

149. Independent Bank's inducement is ongoing.

150. Independent Bank has also indirectly infringed by contributing to the infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Independent Bank has contributed to the direct infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by the end-user of the Accused Instrumentality.

151. The Accused Instrumentality has special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

152. As described above, the special features include securely authorizing specific transactions without providing a credit or debit card number to the merchant used in a manner that infringes the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

153. The special features constitute a material part of the invention of one or more of the claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and are not staple articles of commerce suitable for substantial non-infringing use.

154. Independent Bank's contributory infringement is ongoing.

155. Independent Bank's actions are at least objectively reckless as to the risk of infringing valid patents and this objective risk was either known or should have been known by Independent Bank, at least since the filing of the Complaint.

156. Independent Bank has had knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent at least since the filing of the Complaint.

157. Independent Bank's customers have infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

158. Independent Bank encouraged its customers' infringement.

159. Independent Bank's direct and indirect infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent is, has been, and/or continues to be willful, intentional, deliberate, and/or in conscious disregard of Textile's rights under the patents.

160. Textile has been damaged as a result of the infringing conduct by Independent Bank alleged above. Thus, Independent Bank is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Textile hereby requests a trial by jury on all issues so triable by right.

PRAYER FOR RELIEF

Textile requests that the Court find in its favor and against Independent Bank, and that the Court grant Textile the following relief:

a. Judgment that one or more claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent have been infringed, either literally and/or under the doctrine of equivalents, by Independent Bank and/or all others acting in concert therewith;

b. A permanent injunction enjoining Independent Bank and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert therewith from infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent; or, in the alternative, an award of a reasonable ongoing royalty for future infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent,

and the 454 Patent by such entities;

c. Judgment that Independent Bank account for and pay to Textile all damages to and costs incurred by Textile because of Independent Bank's infringing activities and other conduct complained of herein, including an award of all increased damages to which Textile is entitled under 35 U.S.C. § 284;

d. That Textile be granted pre-judgment and post-judgment interest on the damages caused by Independent Bank's infringing activities and other conduct complained of herein;

e. That this Court declare this an exceptional case and award Textile its reasonable attorney's fees and costs in accordance with 35 U.S.C. § 285; and

f. That Textile be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: October 12, 2021

Respectfully submitted,

/s/ Matthew J. Antonelli

Matthew J. Antonelli

Texas Bar No. 24068432

matt@ahtlawfirm.com

Zachariah S. Harrington

Texas Bar No. 24057886

zac@ahtlawfirm.com

Larry D. Thompson, Jr.

Texas Bar No. 24051428

larry@ahtlawfirm.com

Christopher Ryan Pinckney

Texas Bar No. 24067819

ryan@ahtlawfirm.com

ANTONELLI, HARRINGTON

& THOMPSON LLP

4306 Yoakum Blvd., Ste. 450

Houston, TX 77006

(713) 581-3000

Stafford Davis

State Bar No. 24054605

sdavis@stafforddavisfirm.com

Catherine Bartles
Texas Bar No. 24104849
cbartles@stafforddavisfirm.com
THE STAFFORD DAVIS FIRM
815 South Broadway Avenue
Tyler, Texas 75701
(903) 593-7000
(903) 705-7369 fax

Of Counsel:

Sandeep Seth
Texas State Bar No. 18043000
SETHLAW
Pennzoil Place
700 Milam Street, Suite 1300
Houston, Texas 77002
Telephone: (713) 244-5017
ss@sethlaw.com

Attorneys for Textile Computer Systems, Inc.

EXHIBIT 2F

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

TEXTILE COMPUTER SYSTEMS, INC.,

Plaintiff,

v.

SOUTHSIDE BANK,

Defendant.

CIVIL ACTION NO. 6:21-cv-1056

ORIGINAL COMPLAINT FOR
PATENT INFRINGEMENT

JURY TRIAL DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Textile Computer Systems, Inc. (“Textile” or “Plaintiff”) files this original complaint against Defendant Southside Bank (“Southside”), alleging, based on its own knowledge as to itself and its own actions and based on information and belief as to all other matters, as follows:

PARTIES

1. Textile Computer Systems, Inc. is a corporation formed under the laws of the State of Texas, with a place of business at 618 Bluff Trail, San Antonio, Texas, 78216.
2. Southside Bank is a bank organized and existing under the laws of Texas. Southside Bank has a place of business in Austin, Texas.
3. Southside and its affiliates lead and are part of an interrelated group of companies which together comprise one of the country’s largest banking and financial service entities, including under the Southside brand.
4. Southside and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

5. Southside and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

6. Southside and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

7. Thus, Southside and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

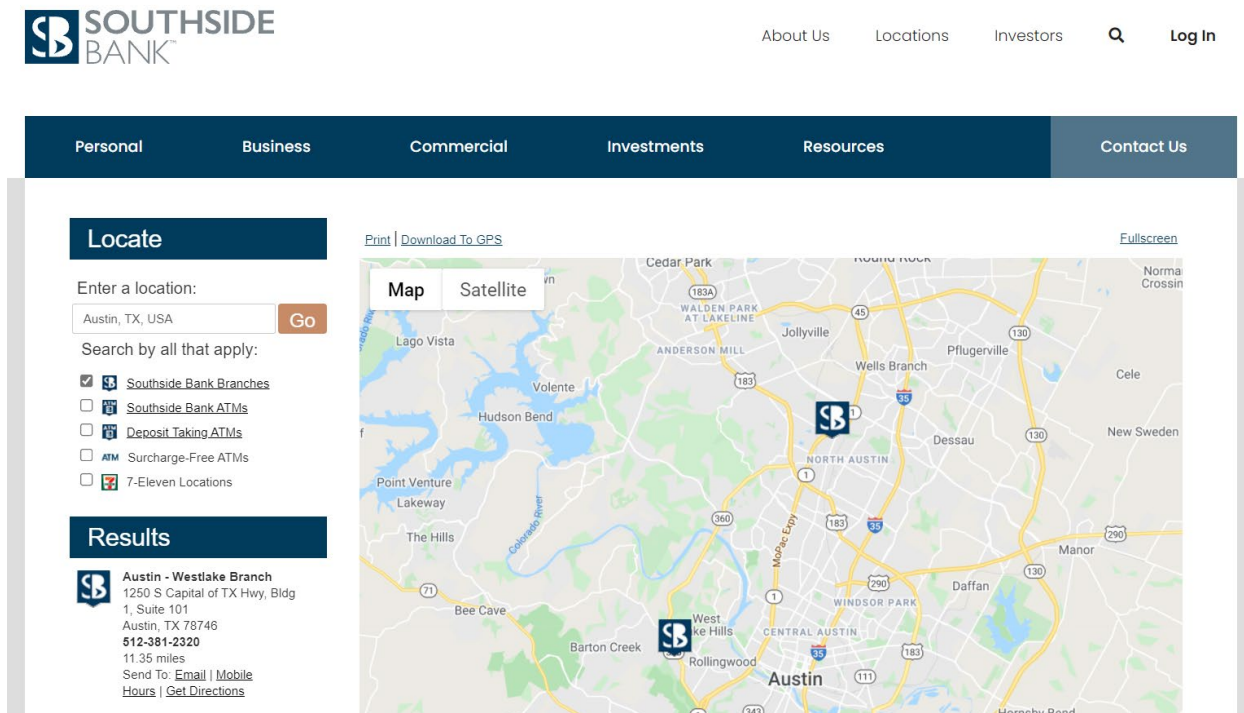
JURISDICTION AND VENUE

8. This is an action for infringement of United States patents arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. § 1331 and § 1338(a).

9. This Court has personal jurisdiction over Southside pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Southside has done and continues to do business in Texas; and (ii) Southside has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations, inducing others to commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein.

10. Venue is proper in this district pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Southside has committed and continues to commit acts of patent infringement in this district. For example, Southside cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those

cardholders make and/or use the accused instrumentalities in the district. Southside induces others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. Southside has regular and established places of business in this district, including at least at 1250 S. Capital of Texas Hwy., Bldg. 1, Suites 101 and 1310, Austin, Texas 78746:



(Source: <https://www.southside.com/locations/>)



(Source: screenshot from Google Maps Street View)

BACKGROUND

11. The patents-in-suit generally pertain to payment authorization technology used in payment networks used to process transactions from, for example, credit cards and debit cards. The technology disclosed by the patents was developed by Gopal Nandakumar, a Texas-based entrepreneur, software engineer, and prolific inventor with over 30 years of experience in the field of Information Management Systems.

12. In 1987, after receiving Master's Degrees from both the University of Madras, India and the Georgia Institute of Technology, Mr. Nandakumar formed Textile Computer Systems, Inc. ("Textile") for the purpose of consulting and developing software for the textile industry. In 2005, Textile began transitioning into credit card transaction systems. In 2011, Textile began to develop and market the MySingleLink suite of applications.

13. The Nandakumar patents are related to payment authorization technology. Mr. Nandakumar has been at the forefront of payment authorization, developing, disclosing, and patenting solutions for reducing fraud in credit and debit card transactions. Indeed, the

Nandakumar patents (or the applications leading to them) have been cited during patent prosecution over a hundred times, including by numerous leading companies in the payment authorization industry such as ADP, Bank of America, Google, Groupon, IBM, Mastercard, NEC, Paypal, Visa, and Wells Fargo.

THE TECHNOLOGY

14. The patents-in-suit, U.S. Patent Nos. 8,505,079, 8,533,802, 9,584,499, 10,148,659, and 10,560,454 (collectively, the “Asserted Patents”), teach systems, including payment processing systems, for securely and effectively approving and processing specific credit card and/or debit card transactions. Through the specific use of servers, messaging gateways, and/or interfaces, these systems act to reduce credit card and/or debit card fraud and misuse through their use and validation of key strings, authentication credentials, transaction specific information, and transaction specific credentials. The technology in the Asserted Patents improves the underlying functionality of existing card processing infrastructure by minimizing fraud and data theft in the face of attacks on payment systems that continue to grow in their number and sophistication.

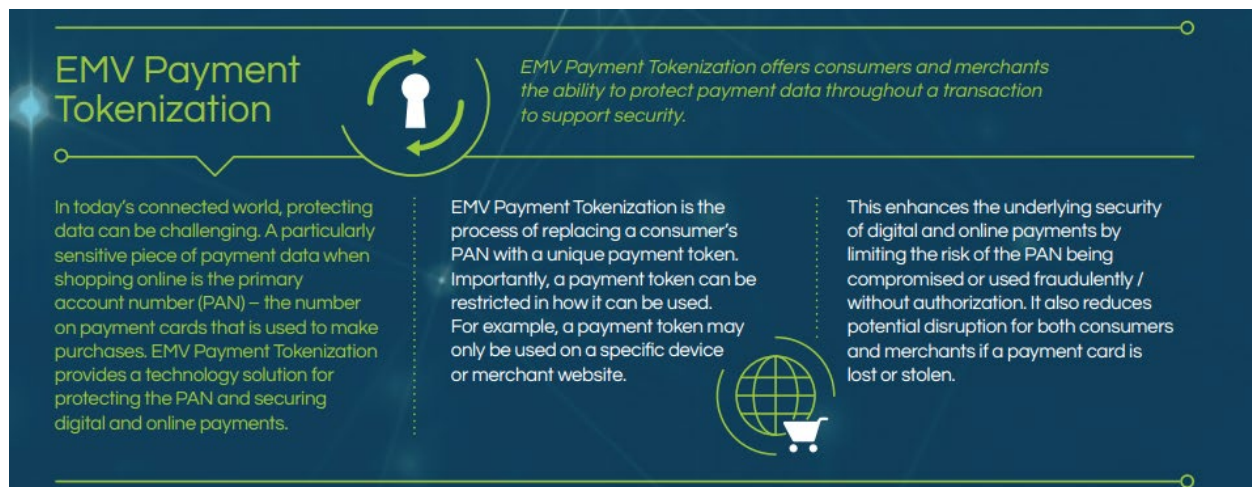
15. The patented improvements are critical for implementing secure payment systems, especially in light of the many high-profile merchant data breaches that have led to increased credit and debit card fraud. For example, in 2006, TJX Companies, who owns retailers like TJMaxx and Marshall’s, was hit with a cyber attack that resulted in the theft of credit cards leading to over \$100 million in fraud losses. In 2013, five people were indicted for attacking a number of retailers and financial institutions including NASDAQ, 7-Eleven, JCP, and others, stealing over 160 million cards. Also in 2013, the retailer Target suffered a data breach that resulted in 40 million debit and credit cards being compromised.

16. One implementation of the technology claimed in the Asserted Patents has been described by EMVCo as “a global Payment Tokenisation ecosystem that overlays and interoperates with existing payment ecosystems to support digital commerce and new methods of payment” and as “enhanc[ing] the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorized or fraudulent use of PANs.”

(Source: <https://www.emvco.com/emv-technologies/payment-tokenisation/>).

17. The technology claimed in the Asserted Patents is far from conventional technology. The payment industry gathered and consulted experts who worked together over a number of years to develop infringing payment tokenisation systems. In other words, the technology claimed in the Asserted Patents was not existing or conventional technology that the payment industry had sitting on the shelf.

18. Indeed, as recently as February of this year, EMVCo itself recognized that an implementation of the technology claimed in the Asserted Patents “provides a technology solution for protecting the PAN and securing digital and online payments”:



(Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

19. That same EMVCo document notes that “In today’s connected world, protecting data can be challenging. A particularly sensitive piece of payment data when shopping online is the primary account number (PAN) – the number on payment cards that is used to make purchases” and that EMVCo’s payment tokenization “enhances the underlying security of digital and online payments by limiting the risk of the PAN being compromised or used fraudulently / without authorization.” The document also states that the “Payment Tokenisation Specification provides an interoperable Technical Framework.” (Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

20. One of the asserted patents, the 079 Patent, was challenged in an Inter Partes Review proceeding before the Patent and Trademark Office (“PTO”). The PTO found that the challenger, Unified Patents Inc., was unable to show that one element, the “key string” as claimed in the 079 Patent claims and as construed by the PTO, was in the prior art at all, much less it being conventional or widespread. The PTO thus confirmed the patentability of all challenged claims of the 079 Patent.

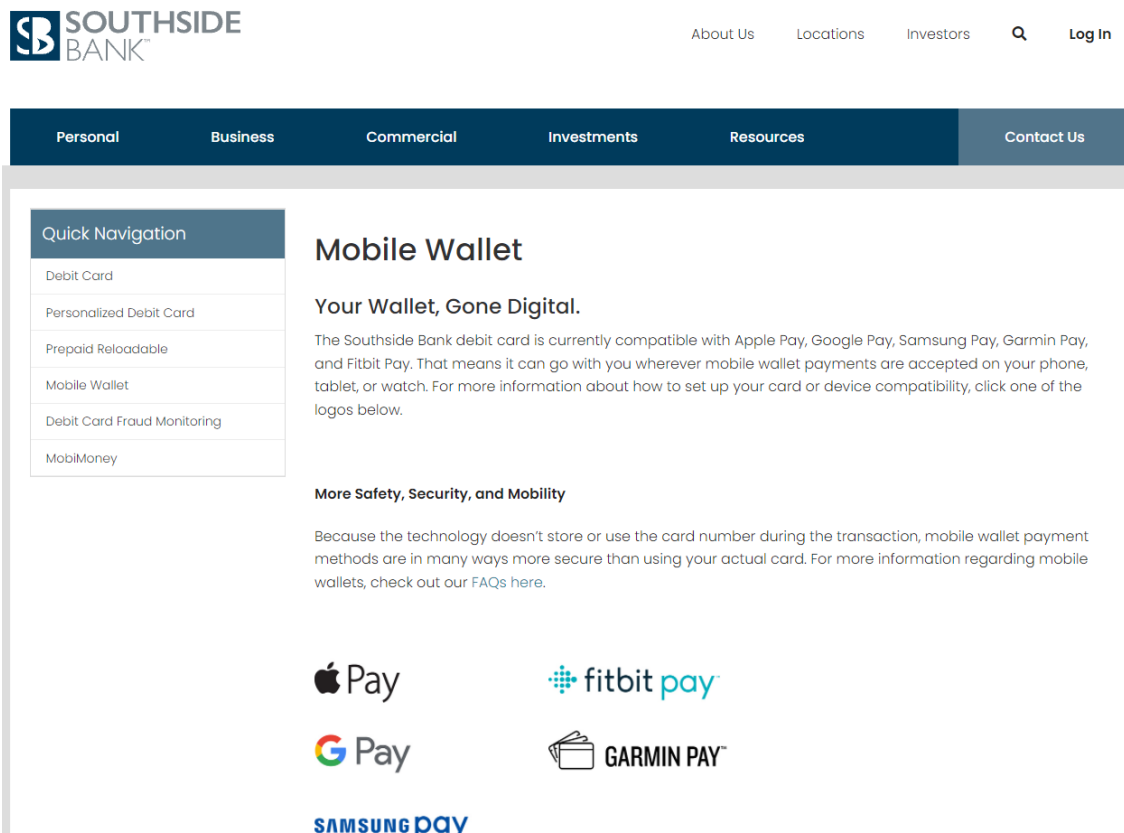
COUNT I

INFRINGEMENT OF U.S. PATENT NO. 8,505,079

21. On August 6, 2013, United States Patent No. 8,505,079 (“the 079 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

22. Textile is the owner of the 079 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 079 Patent against infringers, and to collect damages for all relevant times.

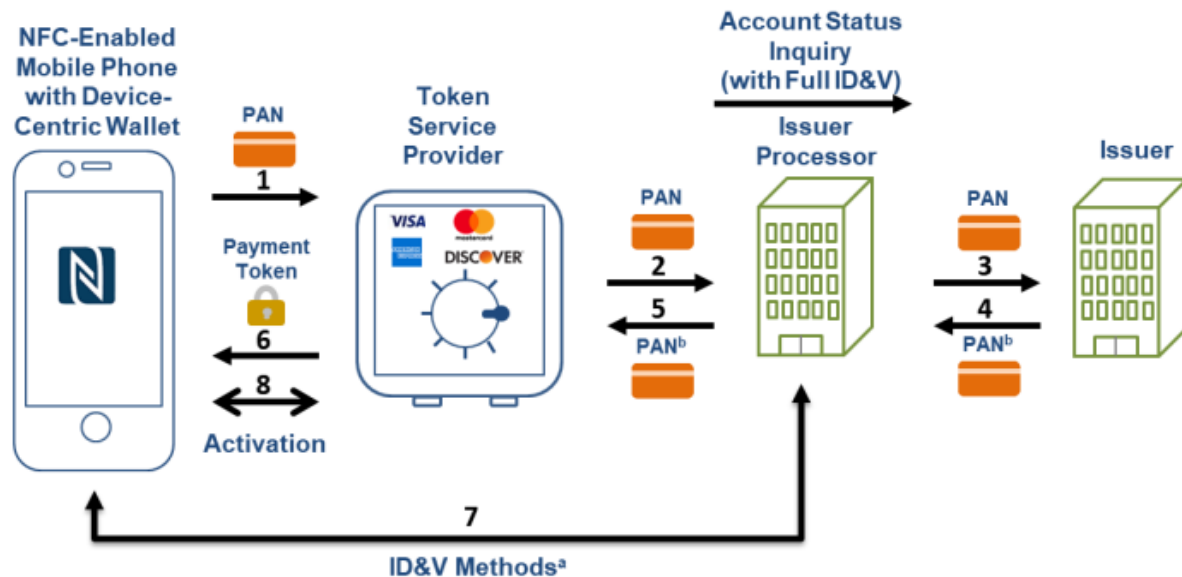
23. Southside offers debit and/or credit cards, such as the Southside Bank Debit Card, that are used with an authentication system that authenticates the identity of a Southside card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Southside card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities, for example. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.



(Source: <https://www.southside.com/personal-banking/cards/mobile-wallet/>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^a ID&V methods includes text or email or call. OTP is an example.

^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

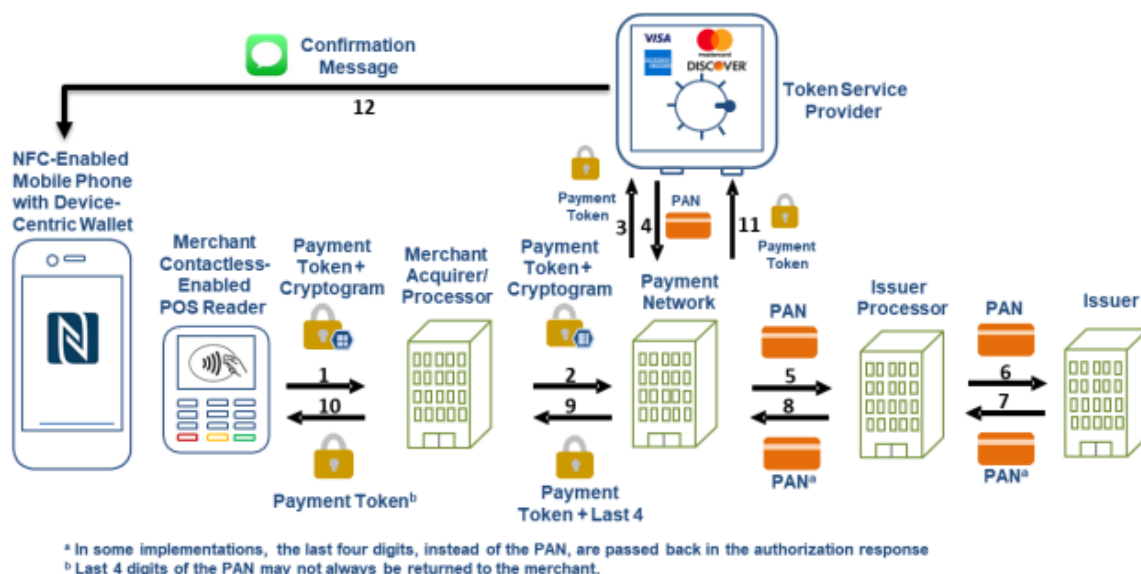


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

24. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a Southside account holder requests Southside to provision a specific Southside debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Southside card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's

smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

25. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Southside card account holders for provisioning a specific Southside debit and/or credit card for use on their mobile devices. The messaging gateway is also programmed to receive requests initiated by Southside card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Southside card account of the account holder. This messaging gateway is either hosted directly by Southside or through an agent with whom Southside has contracted to receive the messages.

26. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to determine a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the messaging

gateway and in secure communication therewith is an authorization server that processes the received request to identify the token value sent for the account selected to be charged that was passed from the authorized user to the merchant terminal via the NFC communication link. From the token value, the server can look up the debit and/or credit card account number. The authorization server is either hosted directly by Southside or through an agent with whom Southside has contracted to provide the authentication services.

27. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive within the payment authorization request transaction specific information that was input into the request by the merchant. The interface is either hosted directly by Southside or through an agent with whom Southside has contracted to provide the authentication services.

28. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

29. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

30. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

31. Defendants thus infringe one or more of the claims of the 079 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 079 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 079 Patent.

32. Southside has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(a), by making, using, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

33. Southside has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 079 Patent by others and Southside will continue to do so unless enjoined by this Court. Southside's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors,

agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 079 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Southside knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 079 Patent.

34. Southside continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 079 Patent.

35. Southside has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 079 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

36. Southside has committed these acts of infringement without license or authorization.

37. By engaging in the conduct described herein, Southside has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Southside is thus liable to Textile for infringement of the 079 Patent, pursuant to 35 U.S.C. § 271.

38. As a direct and proximate result of Southside's infringement of the 079 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Southside's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

39. In addition, the infringing acts and practices of Southside have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Southside is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Southside is finally and permanently enjoined from further infringement.

40. Southside has had actual knowledge of the 079 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Southside will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 079 Patent.

41. Southside has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 079 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

42. Textile has been damaged as a result of the infringing conduct by Southside alleged above. Thus, Southside is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

43. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 079 Patent.

COUNT II

INFRINGEMENT OF U.S. PATENT NO. 8,533,802

44. On September 10, 2013, United States Patent No. 8,533,802 (“the 802 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

45. Textile is the owner of the 802 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 802 Patent against infringers, and to collect damages for all relevant times.

46. Southside offers debit and/or credit cards, such as the Southside Bank Debit Card, that are used with an authentication system that authenticates the identity of a Southside card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Southside card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via

their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.

SOUTHSIDE BANK

About Us Locations Investors Log In

Personal Business Commercial Investments Resources Contact Us

Quick Navigation

- Debit Card
- Personalized Debit Card
- Prepaid Reloadable
- Mobile Wallet
- Debit Card Fraud Monitoring
- MobilMoney

Mobile Wallet

Your Wallet, Gone Digital.

The Southside Bank debit card is currently compatible with Apple Pay, Google Pay, Samsung Pay, Garmin Pay, and Fitbit Pay. That means it can go with you wherever mobile wallet payments are accepted on your phone, tablet, or watch. For more information about how to set up your card or device compatibility, click one of the logos below.

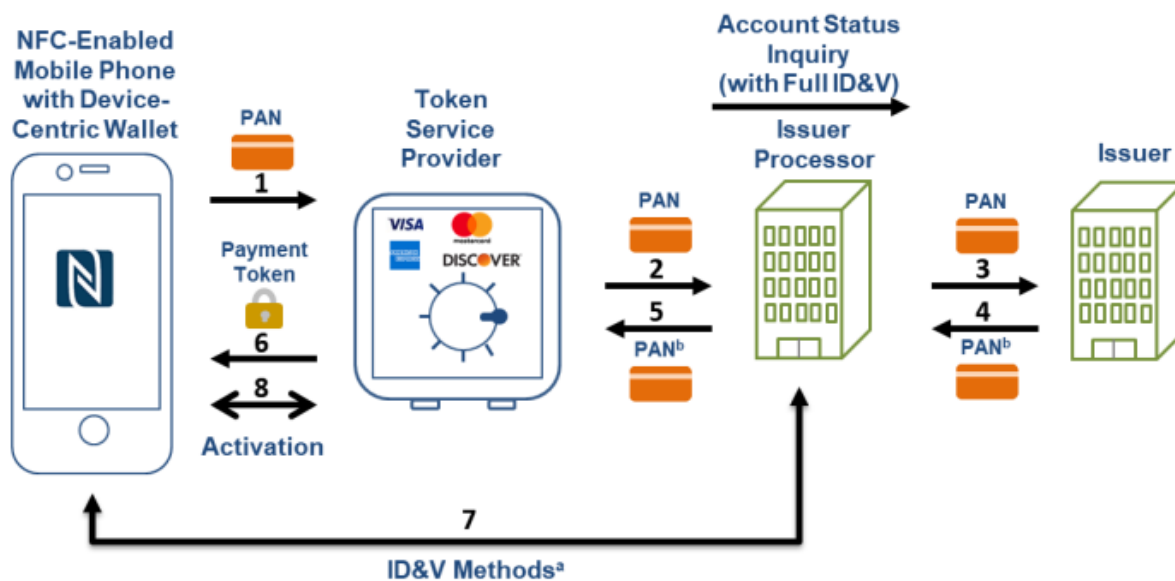
More Safety, Security, and Mobility

Because the technology doesn't store or use the card number during the transaction, mobile wallet payment methods are in many ways more secure than using your actual card. For more information regarding mobile wallets, check out our [FAQs here](#).

(Source: <https://www.southside.com/personal-banking/cards/mobile-wallet/>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

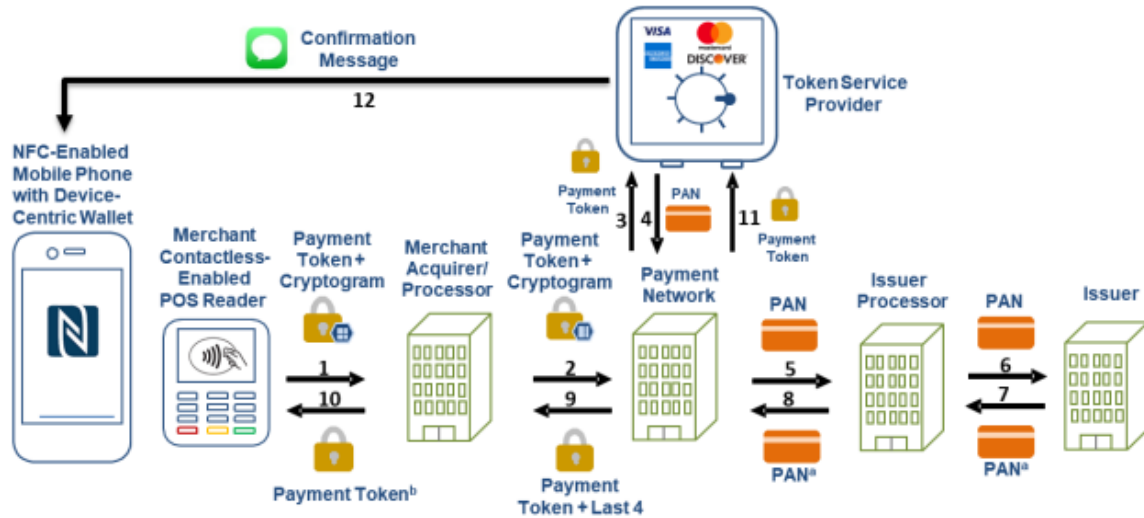
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

47. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a Southside account holder requests Southside to provision a specific Southside debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Southside card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's

smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

48. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Southside card account holders for provisioning a specific Southside debit and/or credit card for use on their mobile devices. This messaging gateway is either hosted directly by Southside or through an agent with whom Southside has contracted to receive the messages.

49. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate a key string adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the message gateway and in secure communication therewith is an authorization server that generates a token corresponding to the debit and/or credit card account number. The authorization server is either hosted directly by Southside or through an agent with whom Southside has contracted to provide the authentication services.

50. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive transaction specific information that was input into the request by the merchant, *e.g.*, the merchant ID, invoice number, invoice amount, and date/timestamp. The interface is either hosted directly by Southside or through an agent with whom Southside has contracted to provide the authentication services.

51. The Accused Instrumentality includes a first set of instructions further operable to communicate the key string to the authorized user that the requester purports to be. For example, the messaging gateway sends the generated token to the authorized user's mobile device for use in merchant transactions.

52. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

53. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

54. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

55. Defendants thus infringe one or more claims of the 802 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 802 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 802 Patents.

56. Southside has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

57. Southside has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 802 Patent by others and Southside will continue to do so unless enjoined by this Court. Southside's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to,

encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 802 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Southside knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 802 Patent.

58. Southside continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 802 Patent.

59. Southside has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 802 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

60. Southside has committed these acts of infringement without license or authorization.

61. By engaging in the conduct described herein, Southside has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Southside is thus liable to Textile for infringement of the 802 Patent, pursuant to 35 U.S.C. § 271.

62. As a direct and proximate result of Southside's infringement of the 802 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Southside's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

63. In addition, the infringing acts and practices of Southside have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Southside is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Southside is finally and permanently enjoined from further infringement.

64. Southside has had actual knowledge of the 802 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Southside will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 802 Patent.

65. Southside has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 802 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

66. Textile has been damaged as a result of the infringing conduct by Southside alleged above. Thus, Southside is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

67. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 802 Patent.

COUNT III

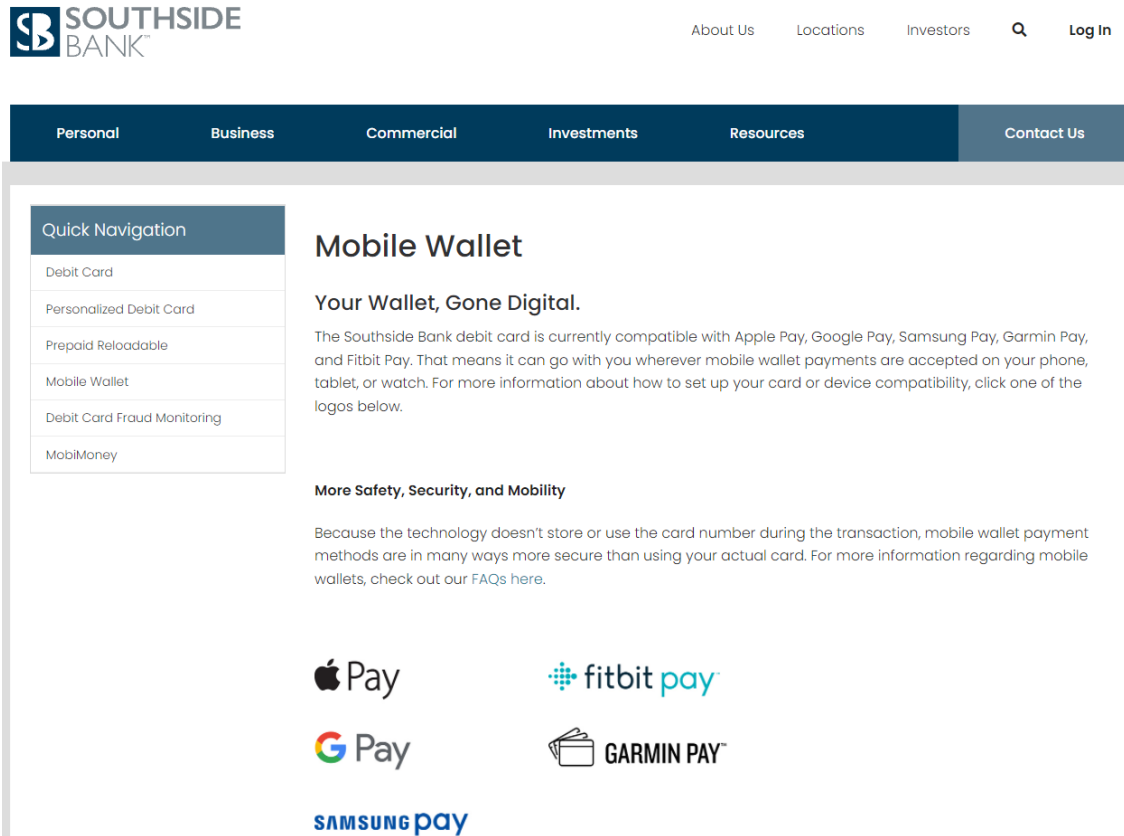
INFRINGEMENT OF U.S. PATENT NO. 9,584,499

68. On February 28, 2017, United States Patent No. 9,584,499 (“the 499 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

69. Textile is the owner of the 499 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 499 Patent against infringers, and to collect damages for all relevant times.

70. Southside offers debit and/or credit cards, such as the Southside Bank Debit Card, that are used by Southside in practicing a method for authorizing transaction specific access to a secured resource having a secured resource identity (the “Accused Instrumentality”). The Southside transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated

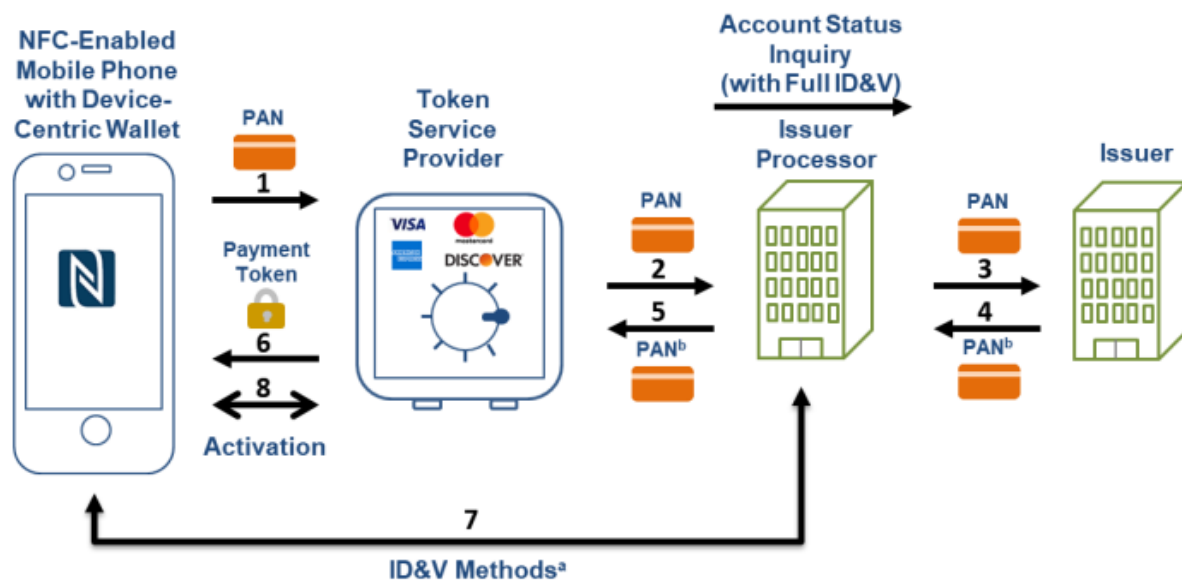
by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



(Source: <https://www.southside.com/personal-banking/cards/mobile-wallet/>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

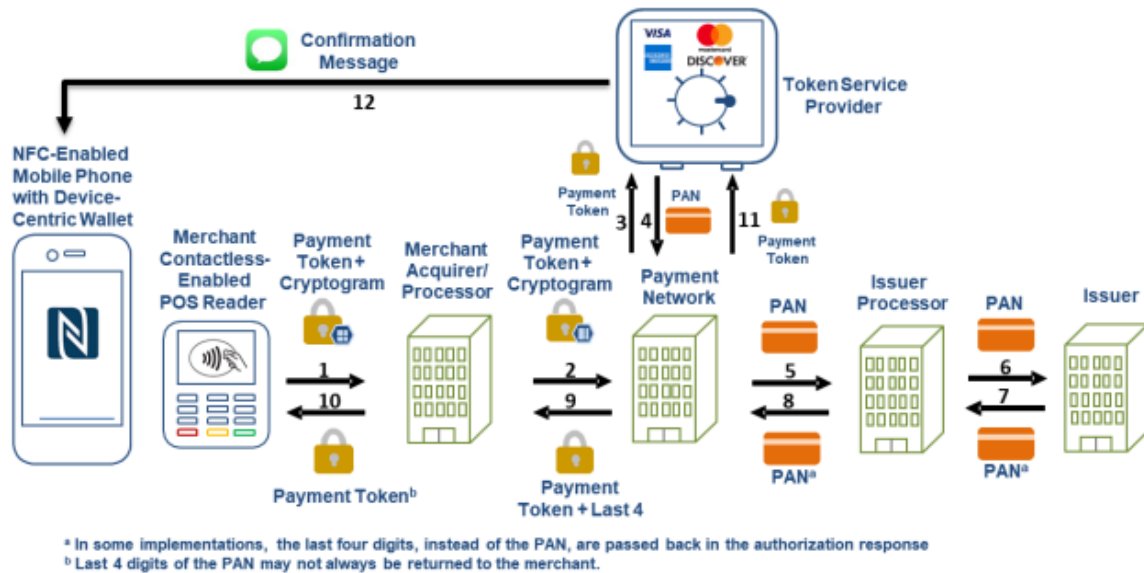


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

71. Southside's use of the Accused Instrumentality includes a method for authorizing transaction specific access to a secured resource having a secured resource identity. For example, a Southside account holder requests Southside to provision a specific Southside debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Southside card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's

smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram.

72. The Accused Instrumentality includes receiving at a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive a request for transaction specific access to a secured resource by a service client. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Southside card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Southside card account of the account holder. This messaging gateway is either hosted directly by Southside or through an agent with whom Southside has contracted to receive the messages.

73. The Accused Instrumentality includes generating a key string with a server in communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate the key string known to both said server and an authorized user of the secured resource, said key string being associated with the secured resource within a key string table accessible by the server and providing a basis for authenticating the secured resource identity by searching the key string table for the key string. For example, behind the firewall of the messaging gateway and in communication therewith is an authorization server that generates a token corresponding to a secured resource during the

provisioning process. After this, the authorization server updates a table that maps token numbers to secured resource identities. The authorization server is then able to search the table to authenticate a secured resource identity by searching the table for the token. If the token has a corresponding secured resource identity, that identity is authenticated. The authorization server is either hosted directly by Southside or through an agent with whom Southside has contracted to provide the authentication services.

74. The Accused Instrumentality includes determining transaction specific information with the server in communication with the messaging gateway, the server having a third set of instructions embodied in a computer readable medium operable to identify transaction specific information within the request. For example, the authorization server is also programmed to identify within the payment authorization request transaction specific information that was passed by the merchant. The authorization server is either hosted directly by Southside or through an agent with whom Southside has contracted to provide the authentication services.

75. The Accused Instrumentality includes communicating said key string to said authorized user. For example, once the provisioning process is complete, the messaging gateway and/or the server send the token to the authorized user's mobile device. The messaging gateway is either hosted directly by Southside or through an agent with whom Southside has contracted to provide the authentication services. The authorization server is either hosted directly by Southside or through an agent with whom Southside has contracted to provide the authentication services.

76. The Accused Instrumentality includes receiving an authentication credential from said service client, said authentication credential having been provided to said service client by

said authorized user. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant. The authorization server is either hosted directly by Southside or through an agent with whom Southside has contracted to provide the authentication services.

77. The Accused Instrumentality includes evaluating said authentication credential. For example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authorizes the transaction specific access. The authorization server is either hosted directly by Southside or through an agent with whom Southside has contracted to provide the authentication services.

78. The Accused Instrumentality includes wherein the key string and authentication credential do not reveal any primary identifier associated with said secured resource. For example, neither the token nor the cryptogram reveals the debit and/or credit card number associated with the secured resource.

79. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

80. Defendants thus infringe one or more claims of the 499 Patent. The elements and conduct described herein are covered by and infringe upon at least Claim 3 of the 499 Patent.

Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 499 Patent.

81. Southside has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

82. Southside has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 499 Patent by others and Southside will continue to do so unless enjoined by this Court. Southside's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 499 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Southside knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 499 Patent.

83. Southside continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers,

businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 499 Patent.

84. Southside has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 499 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

85. Southside has committed these acts of infringement without license or authorization.

86. By engaging in the conduct described herein, Southside has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Southside is thus liable to Textile for infringement of the 499 Patent, pursuant to 35 U.S.C. § 271.

87. As a direct and proximate result of Southside's infringement of the 499 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Southside's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

88. In addition, the infringing acts and practices of Southside have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Southside is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Southside is finally and permanently enjoined from further infringement.

89. Southside has had actual knowledge of the 499 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Southside will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 499 Patent.

90. Southside has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 499 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

91. Textile has been damaged as a result of the infringing conduct by Southside alleged above. Thus, Southside is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

92. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 499 Patent.

COUNT IV

INFRINGEMENT OF U.S. PATENT NO. 10,148,659

93. On December 4, 2018, United States Patent No. 10,148,659 (“the 659 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

94. Textile is the owner of the 659 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 659 Patent against infringers, and to collect damages for all relevant times.

95. Southside offers debit and/or credit cards, such as the Southside Bank Debit Card, that are used with a computer-implemented system for a credit or debit and/or credit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit and/or credit card account number to the merchant (the “Accused Instrumentality”). The Southside transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.


[About Us](#)
[Locations](#)
[Investors](#)

[Log In](#)
[Personal](#)
[Business](#)
[Commercial](#)
[Investments](#)
[Resources](#)
[Contact Us](#)

Quick Navigation

[Debit Card](#)
[Personalized Debit Card](#)
[Prepaid Reloadable](#)
[Mobile Wallet](#)
[Debit Card Fraud Monitoring](#)
[MobiMoney](#)

Mobile Wallet

Your Wallet, Gone Digital.

The Southside Bank debit card is currently compatible with Apple Pay, Google Pay, Samsung Pay, Garmin Pay, and Fitbit Pay. That means it can go with you wherever mobile wallet payments are accepted on your phone, tablet, or watch. For more information about how to set up your card or device compatibility, click one of the logos below.

More Safety, Security, and Mobility

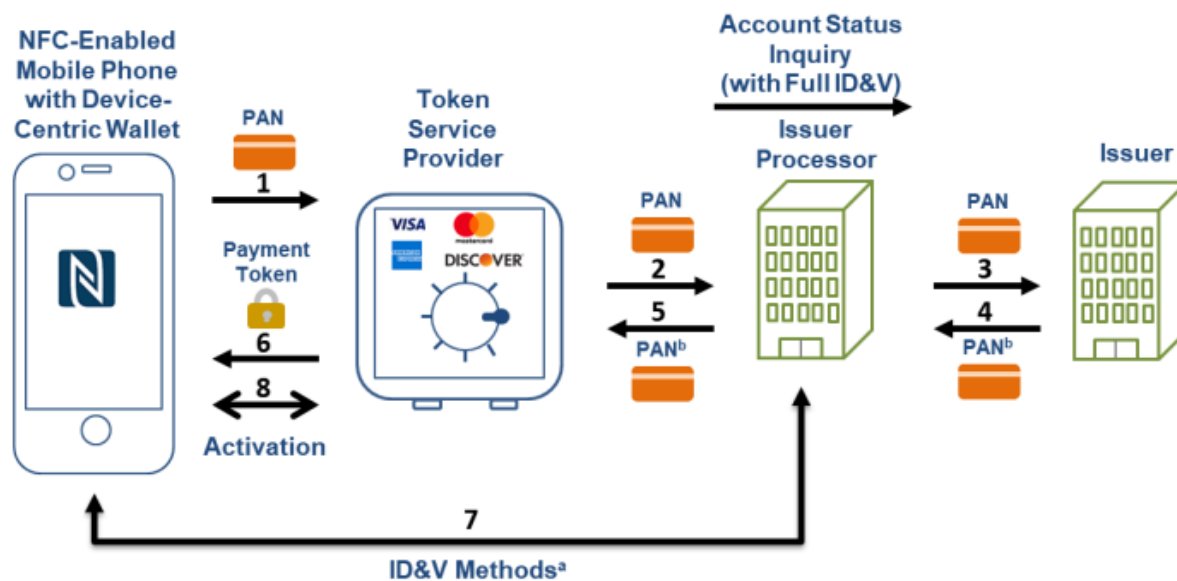
Because the technology doesn't store or use the card number during the transaction, mobile wallet payment methods are in many ways more secure than using your actual card. For more information regarding mobile wallets, check out our [FAQs here](#).



(Source: <https://www.southside.com/personal-banking/cards/mobile-wallet/>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

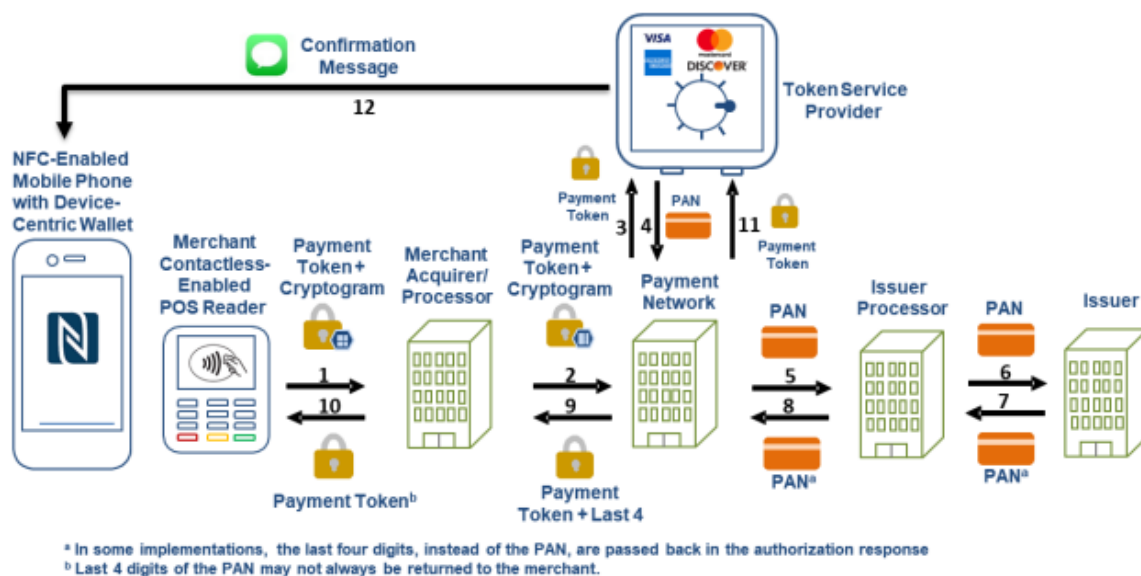


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

96. The Accused Instrumentality includes a computer-implemented system for a credit or debit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit card account number to the merchant. For example, a Southside account holder requests Southside to provision a specific Southside debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Southside to a specific merchant in a specific amount for a specific transaction from a specific

Southside card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

97. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a credit or debit card account holder's mobile device, a merchant's payment application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a Southside card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Southside card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Southside card account of the account holder. This interface is either hosted directly by Southside or through an agent with whom Southside has contracted to receive the messages.

98. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration

information received from the credit or debit card account holder through the at least one interface, the registration information comprising a credit or debit card account holder identifier and at least one credit or debit card account number having an associated unique account identifier wherein the credit or debit card account number and unique account identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card and the debit and/or credit card account number (which has a corresponding token), received from Southside card account holders through the interface for provisioning a specific Southside debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Southside card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Southside card account of the account holder. The server is either hosted directly by Southside or through an agent with whom Southside has contracted to receive the messages.

99. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to pay the specific merchant for the specific transaction from a given debit or credit card account, the authorization request message having been received through the at least one interface and originating from the credit or debit card account holder's mobile device and comprising: a first merchant identifier; a first transaction specific information selected from the group consisting of a first transaction amount and first client reference identifier; the credit or debit card account holder identifier; and a designated unique account identifier selected from the at least one unique account identifiers. For example, the Accused

Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Southside card account holder's mobile device. The server is programmed to receive authorization requests initiated by Southside card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a merchant identifier, and the Southside card account holder identifier. The server is either hosted directly by Southside or through an agent with whom Southside has contracted to receive the messages.

100. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string wherein the key string is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the designated unique account identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Southside or through an agent with whom Southside has contracted to receive the messages.

101. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive a payment request message from the merchant's payment application through the at least one interface, the payment request message comprising: a second merchant identifier; a second transaction specific information selected from the group consisting of a second transaction amount and second client reference identifier; and a second transaction specific authentication credential whereby the second authentication credential was received by the merchant application from the credit or debit card account holder's mobile device. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Southside card account holder's mobile device. The server is either hosted directly by Southside or through an agent with whom Southside has contracted to receive the messages.

102. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the credit or debit card account holder's request to use the credit or debit card account number associated with the designated unique account identifier for payment to the specific merchant for the specific transaction and authorizing the resource provider to use the credit or debit card account number associated with the designated unique account identifier to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or bank account number to the

specific merchant by determining if: the first merchant identifier matches the second merchant identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Southside or through an agent with whom Southside has contracted to provide the authentication services.

103. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

104. Defendants thus infringe one or more claims of the 659 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 9 of the 659 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 659 Patent.

105. Southside has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C.

§ 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

106. Southside has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 659 Patent by others and Southside will continue to do so unless enjoined by this Court. Southside's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 659 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Southside knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 659 Patent.

107. Southside continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 659 Patent.

108. Southside has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 9 of the 659 Patent, in violation of 35 U.S.C.

§ 271(c), by contributing to the direct infringement of the 659 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

109. Southside has committed these acts of infringement without license or authorization.

110. By engaging in the conduct described herein, Southside has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Southside is thus liable to Textile for infringement of the 659 Patent, pursuant to 35 U.S.C. § 271.

111. As a direct and proximate result of Southside's infringement of the 659 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Southside's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

112. In addition, the infringing acts and practices of Southside have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Southside is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such,

Textile is entitled to compensation for any continuing and/or future infringement up until the date that Southside is finally and permanently enjoined from further infringement.

113. Southside has had actual knowledge of the 659 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Southside will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 659 Patent.

114. Southside has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 659 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

115. Textile has been damaged as a result of the infringing conduct by Southside alleged above. Thus, Southside is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

116. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 659 Patent.

COUNT V

INFRINGEMENT OF U.S. PATENT NO. 10,560,454

117. On February 11, 2020, United States Patent No. 10,560,454 (“the 454 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

118. Textile is the owner of the 454 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 454 Patent against infringers, and to collect damages for all relevant times.

119. Southside offers debit and/or credit cards, such as the Southside Bank Debit Card, that are used with a computer-implemented system for a user to authorize a resource authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client (the "Accused Instrumentality"). The Southside transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.


[About Us](#)
[Locations](#)
[Investors](#)

[Log In](#)
[Personal](#)
[Business](#)
[Commercial](#)
[Investments](#)
[Resources](#)
[Contact Us](#)

Quick Navigation

[Debit Card](#)
[Personalized Debit Card](#)
[Prepaid Reloadable](#)
[Mobile Wallet](#)
[Debit Card Fraud Monitoring](#)
[MobiMoney](#)

Mobile Wallet

Your Wallet, Gone Digital.

The Southside Bank debit card is currently compatible with Apple Pay, Google Pay, Samsung Pay, Garmin Pay, and Fitbit Pay. That means it can go with you wherever mobile wallet payments are accepted on your phone, tablet, or watch. For more information about how to set up your card or device compatibility, click one of the logos below.

More Safety, Security, and Mobility

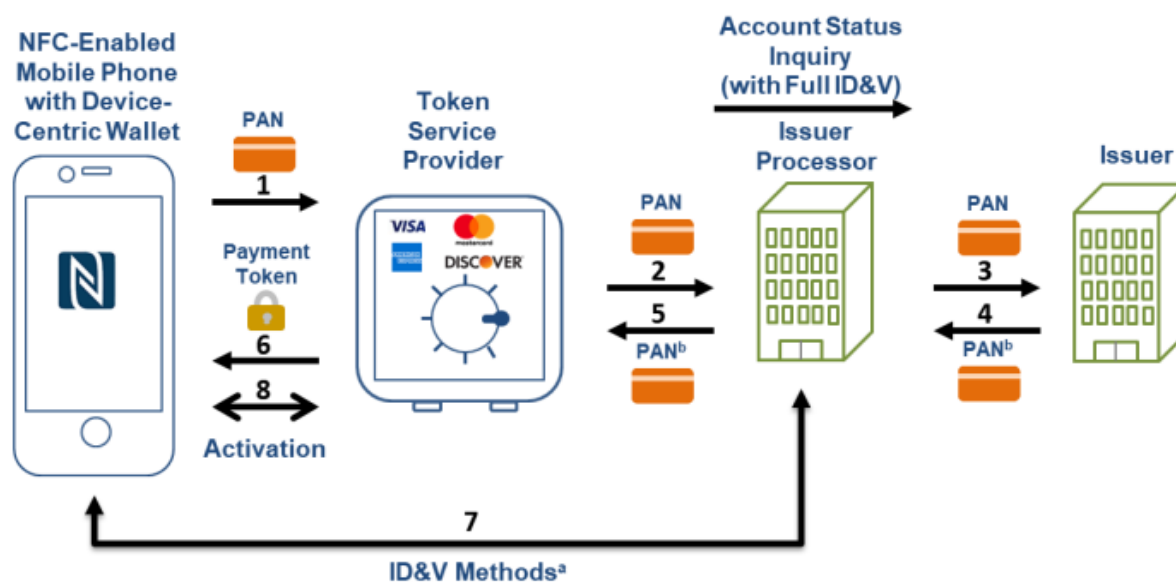
Because the technology doesn't store or use the card number during the transaction, mobile wallet payment methods are in many ways more secure than using your actual card. For more information regarding mobile wallets, check out our [FAQs here](#).



(Source: <https://www.southside.com/personal-banking/cards/mobile-wallet/>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

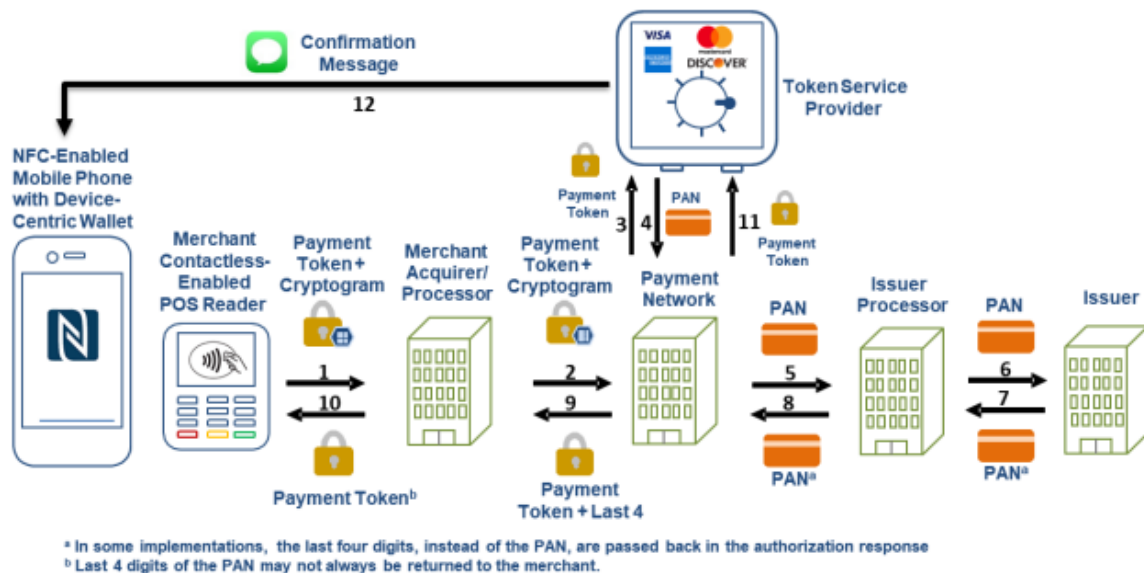


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

120. The Accused Instrumentality includes a computer-implemented system for a user to authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client. For example, a Southside account holder requests Southside to provision a specific Southside debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Southside to a specific merchant in a specific amount for a specific transaction from a specific Southside card account of the account holder

using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

121. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a user's application, a service client's application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a Southside card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Southside card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Southside card account of the account holder. This interface is either hosted directly by Southside or through an agent with whom Southside has contracted to receive the messages.

122. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration information received from the user through the at least one interface, the registration information comprising a user identifier and at least one secured resource identifier associated with the

common identifier of the secured resource, wherein the common identifier and secured resource identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card, the debit and/or credit card account number (which has a corresponding token), and the CVV number received from Southside card account holders through the interface for provisioning a specific Southside debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Southside card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Southside card account of the account holder. The server is either hosted directly by Southside or through an agent with whom Southside has contracted to receive the messages.

123. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to authorize access to the secured resource by the service client, the authorization request message having been received through the at least one interface from the user's application and comprising: a first service client identifier; a first transaction specific information; the user identifier; and a designated secured resource identifier selected from one of the at least one secured resource identifiers. For example, the Accused Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Southside card account holder's mobile device. The server is programmed to receive authorization requests initiated by Southside card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction,

a token, a CVV number, a merchant identifier, other token information, and the Southside card account holder identifier. The server is either hosted directly by Southside or through an agent with whom Southside has contracted to receive the messages.

124. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string and does not include or reveal the common identifier associated with the designated secured resource identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Southside or through an agent with whom Southside has contracted to receive the messages.

125. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive an access request message from the service client's application through the at least one interface, the payment request message comprising: a second service client identifier; a second transaction specific information; and a second transaction specific authentication credential whereby the second transaction specific authentication credential was received by the service client's

application from the user's application. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Southside card account holder's mobile device. The server is either hosted directly by Southside or through an agent with whom Southside has contracted to receive the messages.

126. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the user's request to access the secured resource associated with the designated secured resource identifier without transmitting or otherwise providing the common identifier of the secured resource to the service client by determining if: the first service client identifier matches the second service client identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Southside or through an agent with whom Southside has contracted to provide the authentication services.

127. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

128. Defendants thus infringe one or more claims of the 454 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 8 of the 454 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 454 Patent.

129. Southside has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

130. Southside has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 454 Patent by others and Southside will continue to do so unless enjoined by this Court. Southside's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for

another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 454 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Southside knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 454 Patent.

131. Southside continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 454 Patent.

132. Southside has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 454 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

133. Southside has committed these acts of infringement without license or authorization.

134. By engaging in the conduct described herein, Southside has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Southside is thus liable to Textile for infringement of the 454 Patent, pursuant to 35 U.S.C. § 271.

135. As a direct and proximate result of Southside's infringement of the 454 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Southside's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

136. In addition, the infringing acts and practices of Southside have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Southside is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Southside is finally and permanently enjoined from further infringement.

137. Southside has had actual knowledge of the 454 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Southside will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 454 Patent.

138. Southside has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 454 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

139. Textile has been damaged as a result of the infringing conduct by Southside alleged above. Thus, Southside is liable to Textile in an amount that adequately compensates it

for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

140. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 454 Patent.

ADDITIONAL ALLEGATIONS REGARDING INFRINGEMENT

141. Southside has also indirectly infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by inducing others to directly infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Southside has induced the end-users, Southside's customers, to directly infringe (literally and/or under the doctrine of equivalents) the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by using the Accused Instrumentality.

142. Southside took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

143. Such steps by Southside included, among other things, advising or directing customers and end-users to use the Accused Instrumentality in an infringing manner; advertising and promoting the use of the Accused Instrumentality in an infringing manner; and/or distributing instructions that guide users to use the Accused Instrumentality in an infringing manner.

144. Southside has performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454

Patent and with the knowledge that the induced acts constitute infringement, at least since the filing of the Complaint.

145. Southside was and is aware that the normal and customary use of the Accused Instrumentality by Southside's customers would infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Southside's inducement is ongoing.

146. Southside directs or controls the use of the Accused Instrumentality nationwide through its own websites and in its own branches, including in Texas and elsewhere in the United States, and expects and intends that the Accused Instrumentality will be so used.

147. Southside took active steps, directly and/or through contractual relationships with others, with the specific intent to cause such persons to make or use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

148. Southside performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts would constitute infringement.

149. Southside's inducement is ongoing.

150. Southside has also indirectly infringed by contributing to the infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Southside has contributed to the direct infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by the end-user of the Accused Instrumentality.

151. The Accused Instrumentality has special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the 079

Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

152. As described above, the special features include securely authorizing specific transactions without providing a credit or debit card number to the merchant used in a manner that infringes the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

153. The special features constitute a material part of the invention of one or more of the claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and are not staple articles of commerce suitable for substantial non-infringing use.

154. Southside's contributory infringement is ongoing.

155. Southside's actions are at least objectively reckless as to the risk of infringing valid patents and this objective risk was either known or should have been known by Southside, at least since the filing of the Complaint.

156. Southside has had knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent at least since the filing of the Complaint.

157. Southside's customers have infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

158. Southside encouraged its customers' infringement.

159. Southside's direct and indirect infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent is, has been, and/or continues to be willful, intentional, deliberate, and/or in conscious disregard of Textile's rights under the patents.

160. Textile has been damaged as a result of the infringing conduct by Southside alleged above. Thus, Southside is liable to Textile in an amount that adequately compensates it

for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Textile hereby requests a trial by jury on all issues so triable by right.

PRAYER FOR RELIEF

Textile requests that the Court find in its favor and against Southside, and that the Court grant Textile the following relief:

- a. Judgment that one or more claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent have been infringed, either literally and/or under the doctrine of equivalents, by Southside and/or all others acting in concert therewith;
- b. A permanent injunction enjoining Southside and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert therewith from infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent; or, in the alternative, an award of a reasonable ongoing royalty for future infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by such entities;
- c. Judgment that Southside account for and pay to Textile all damages to and costs incurred by Textile because of Southside's infringing activities and other conduct complained of herein, including an award of all increased damages to which Textile is entitled under 35 U.S.C. § 284;
- d. That Textile be granted pre-judgment and post-judgment interest on the damages caused by Southside's infringing activities and other conduct complained of herein;
- e. That this Court declare this an exceptional case and award Textile its reasonable

attorney's fees and costs in accordance with 35 U.S.C. § 285; and

f. That Textile be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: October 12, 2021

Respectfully submitted,

/s/ Matthew J. Antonelli

Matthew J. Antonelli

Texas Bar No. 24068432

matt@ahtlawfirm.com

Zachariah S. Harrington

Texas Bar No. 24057886

zac@ahtlawfirm.com

Larry D. Thompson, Jr.

Texas Bar No. 24051428

larry@ahtlawfirm.com

Christopher Ryan Pinckney

Texas Bar No. 24067819

ryan@ahtlawfirm.com

ANTONELLI, HARRINGTON

& THOMPSON LLP

4306 Yoakum Blvd., Ste. 450

Houston, TX 77006

(713) 581-3000

Stafford Davis

State Bar No. 24054605

sdavis@stafforddavisfirm.com

Catherine Bartles

Texas Bar No. 24104849

cbartles@stafforddavisfirm.com

THE STAFFORD DAVIS FIRM

815 South Broadway Avenue

Tyler, Texas 75701

(903) 593-7000

(903) 705-7369 fax

Of Counsel:

Sandeep Seth

Texas State Bar No. 18043000

SETHLAW

Pennzoil Place

700 Milam Street, Suite 1300

Houston, Texas 77002
Telephone: (713) 244-5017
ss@sethlaw.com

Attorneys for Textile Computer Systems, Inc.

EXHIBIT 2G

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

TEXTILE COMPUTER SYSTEMS, INC.,

Plaintiff,

v.

TEXAS CAPITAL BANK,

Defendant.

CIVIL ACTION NO. 6:21-cv-1057

ORIGINAL COMPLAINT FOR
PATENT INFRINGEMENT

JURY TRIAL DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Textile Computer Systems, Inc. (“Textile” or “Plaintiff”) files this original complaint against Defendant Texas Capital Bank (“Texas Capital”), alleging, based on its own knowledge as to itself and its own actions and based on information and belief as to all other matters, as follows:

PARTIES

1. Textile Computer Systems, Inc. is a corporation formed under the laws of the State of Texas, with a place of business at 618 Bluff Trail, San Antonio, Texas, 78216.
2. Texas Capital Bank is a bank organized and existing under the laws of Texas. Texas Capital Bank has places of business in Austin, Texas and San Antonio, Texas.
3. Texas Capital and its affiliates lead and are part of an interrelated group of companies which together comprise one of the country’s largest banking and financial service entities, including under the Texas Capital brand.
4. Texas Capital and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

5. Texas Capital and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

6. Texas Capital and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

7. Thus, Texas Capital and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

JURISDICTION AND VENUE

8. This is an action for infringement of United States patents arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. § 1331 and § 1338(a).

9. This Court has personal jurisdiction over Texas Capital pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Texas Capital has done and continues to do business in Texas; and (ii) Texas Capital has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations, inducing others to commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein.

10. Venue is proper in this district pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Texas Capital has committed and continues to commit acts of patent infringement in this district. For example, Texas Capital cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment

systems, those cardholders make and/or use the accused instrumentalities in the district. Texas Capital induces others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. Texas Capital has regular and established places of business in this district, including at least at 7373 Broadway, Suite 100, San Antonio, Texas 78209, at 98 San Jacinto Blvd., Suite 150, Austin, Texas 78701, and at numerous other locations in San Antonio and Austin:

TEXAS CAPITAL BANK Commercial Banking Wealth Management Who We Are

Our Company ▼ People ▼ Locations Investor Relations Newsroom Careers

← LOCATIONS

Our Locations

Texas Capital Bank provides commercial banking expertise and highly personalized financial services to businesses across the country.

AUSTIN DALLAS FORT WORTH HOUSTON SAN ANTONIO NEW YORK

San Antonio

LOBBY HOURS:
Monday - Thursday
9 a.m. - 4 p.m.
Friday
9 a.m. - 5 p.m.

2
Quarry Heights Banking Center
7373 Broadway Street
Suite 100
San Antonio, Texas 78209

Map **Satellite**

Quarry Heights Banking Center
7373 Broadway, Suite 100
San Antonio, Texas 78209

DIRECTIONS

PHONE: 210-283-5220
FAX: 210-283-5240

DRIVE-THRU HOURS:
Monday - Friday
8 a.m. - 5 p.m.

(Source: <https://www.texascapitalbank.com/who-we-are/locations/san-antonio>)



(Source: screenshot from Google Maps Street View)

CONTACT US

LOG IN

Texas Capital Bank

Commercial Banking

Wealth Management

Who We Are

Our Company

People

Locations

Investor Relations

Newsroom

Careers

← LOCATIONS

Our Locations

Texas Capital Bank provides commercial banking expertise and highly personalized financial services to businesses across the country.

AUSTIN

DALLAS

FORT WORTH

HOUSTON

SAN ANTONIO

NEW YORK

Austin

Executive Office

98 San Jacinto Blvd.
Suite 200
Austin, Texas 78701

DIRECTIONS

PHONE: 512.305.4000
FAX: 512.305.4001

1

Banking Center

98 San Jacinto Blvd.
Suite 150
Austin, Texas 78701

Map

Satellite

(Source: <https://www.texascapitalbank.com/who-we-are/locations/austin>)

4



(Source: screenshot from Google Maps Street View)

BACKGROUND

11. The patents-in-suit generally pertain to payment authorization technology used in payment networks used to process transactions from, for example, credit cards and debit cards. The technology disclosed by the patents was developed by Gopal Nandakumar, a Texas-based entrepreneur, software engineer, and prolific inventor with over 30 years of experience in the field of Information Management Systems.

12. In 1987, after receiving Master's Degrees from both the University of Madras, India and the Georgia Institute of Technology, Mr. Nandakumar formed Textile Computer Systems, Inc. ("Textile") for the purpose of consulting and developing software for the textile industry. In 2005, Textile began transitioning into credit card transaction systems. In 2011, Textile began to develop and market the MySingleLink suite of applications.

13. The Nandakumar patents are related to payment authorization technology. Mr. Nandakumar has been at the forefront of payment authorization, developing, disclosing, and patenting solutions for reducing fraud in credit and debit card transactions. Indeed, the

Nandakumar patents (or the applications leading to them) have been cited during patent prosecution over a hundred times, including by numerous leading companies in the payment authorization industry such as ADP, Bank of America, Google, Groupon, IBM, Mastercard, NEC, Paypal, Visa, and Wells Fargo.

THE TECHNOLOGY

14. The patents-in-suit, U.S. Patent Nos. 8,505,079, 8,533,802, 9,584,499, 10,148,659, and 10,560,454 (collectively, the “Asserted Patents”), teach systems, including payment processing systems, for securely and effectively approving and processing specific credit card and/or debit card transactions. Through the specific use of servers, messaging gateways, and/or interfaces, these systems act to reduce credit card and/or debit card fraud and misuse through their use and validation of key strings, authentication credentials, transaction specific information, and transaction specific credentials. The technology in the Asserted Patents improves the underlying functionality of existing card processing infrastructure by minimizing fraud and data theft in the face of attacks on payment systems that continue to grow in their number and sophistication.

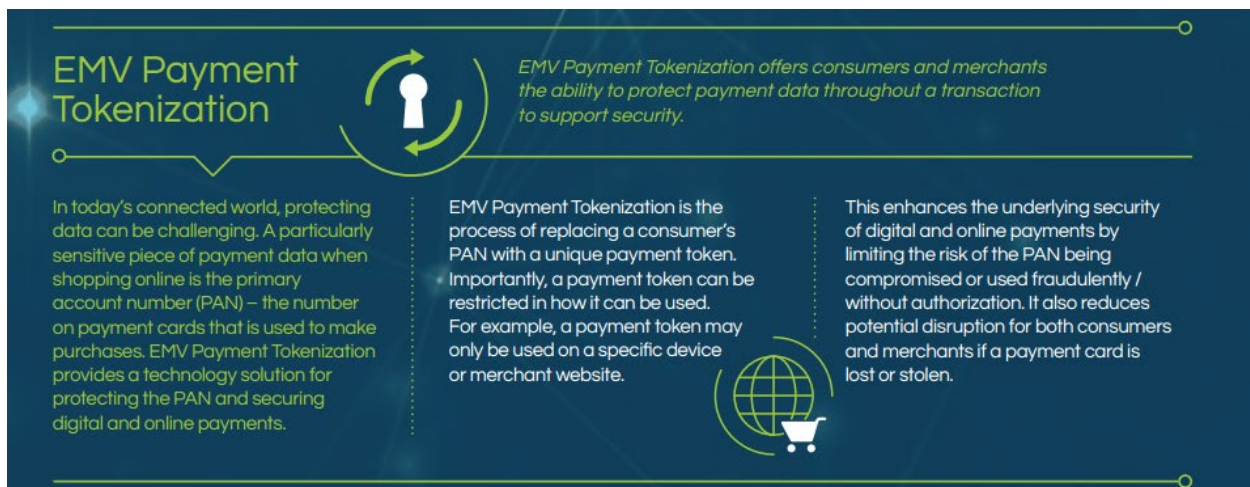
15. The patented improvements are critical for implementing secure payment systems, especially in light of the many high-profile merchant data breaches that have led to increased credit and debit card fraud. For example, in 2006, TJX Companies, who owns retailers like TJMaxx and Marshall’s, was hit with a cyber attack that resulted in the theft of credit cards leading to over \$100 million in fraud losses. In 2013, five people were indicted for attacking a number of retailers and financial institutions including NASDAQ, 7-Eleven, JCP, and others, stealing over 160 million cards. Also in 2013, the retailer Target suffered a data breach that resulted in 40 million debit and credit cards being compromised.

16. One implementation of the technology claimed in the Asserted Patents has been described by EMVCo as “a global Payment Tokenisation ecosystem that overlays and interoperates with existing payment ecosystems to support digital commerce and new methods of payment” and as “enhanc[ing] the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorized or fraudulent use of PANs.”

(Source: <https://www.emvco.com/emv-technologies/payment-tokenisation/>).

17. The technology claimed in the Asserted Patents is far from conventional technology. The payment industry gathered and consulted experts who worked together over a number of years to develop infringing payment tokenisation systems. In other words, the technology claimed in the Asserted Patents was not existing or conventional technology that the payment industry had sitting on the shelf.

18. Indeed, as recently as February of this year, EMVCo itself recognized that an implementation of the technology claimed in the Asserted Patents “provides a technology solution for protecting the PAN and securing digital and online payments”:



(Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

19. That same EMVCo document notes that “In today’s connected world, protecting data can be challenging. A particularly sensitive piece of payment data when shopping online is the primary account number (PAN) – the number on payment cards that is used to make purchases” and that EMVCo’s payment tokenization “enhances the underlying security of digital and online payments by limiting the risk of the PAN being compromised or used fraudulently / without authorization.” The document also states that the “Payment Tokenisation Specification provides an interoperable Technical Framework.” (Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

20. One of the asserted patents, the 079 Patent, was challenged in an Inter Partes Review proceeding before the Patent and Trademark Office (“PTO”). The PTO found that the challenger, Unified Patents Inc., was unable to show that one element, the “key string” as claimed in the 079 Patent claims and as construed by the PTO, was in the prior art at all, much less it being conventional or widespread. The PTO thus confirmed the patentability of all challenged claims of the 079 Patent.

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 8,505,079

21. On August 6, 2013, United States Patent No. 8,505,079 (“the 079 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

22. Textile is the owner of the 079 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 079 Patent against infringers, and to collect damages for all relevant times.

23. Texas Capital offers debit and/or credit cards, such as the Texas Capital Visa Debit Cards, that are used with an authentication system that authenticates the identity of a Texas Capital card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Texas Capital card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities, for example. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.

Debit Card Solutions

All Texas Capital Bank checking accounts come with a Visa® Debit Card with embedded chip technology as well as magnetic stripe functionality. Features include:

Enjoy an easier way of paying in stores or within apps with [Apple Pay](#)®, [Samsung Pay](#)®, and [Google Pay](#)®

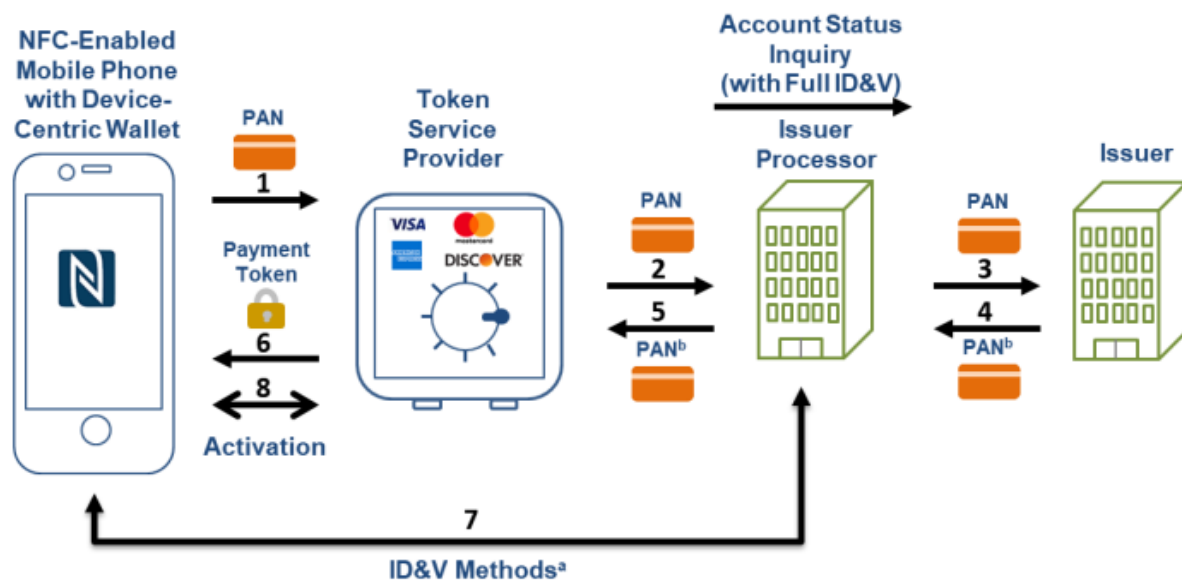
Fraud Protection: We rely on the latest technology and strategies to protect your account from fraud:

- **CardValet:** Manage your debit card usage through your mobile device by defining when, where and how your payment card is used with CardValet. [Learn more about CardValet.](#)
- **Chip Technology:** When your card is used at a chip card reader, each transaction generates a unique, one-time code, providing an added layer of security.
- **Limits:** For added protection, your card provides a daily \$4,000 point of sale limit, along with a daily ATM limit of \$500.
- **Real-Time Fraud Monitoring:** When debit card transactions fall out of your normal spending patterns, we’ll contact you to make sure the transaction is actually yours.
- **Visa® Zero Liability Protection:** With [Visa Secure](#), you’re not liable for any unauthorized debit card transactions when you notify the bank promptly.

(Source: <https://www.texascapitalbank.com/personal-banking/debit-credit-card-services>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

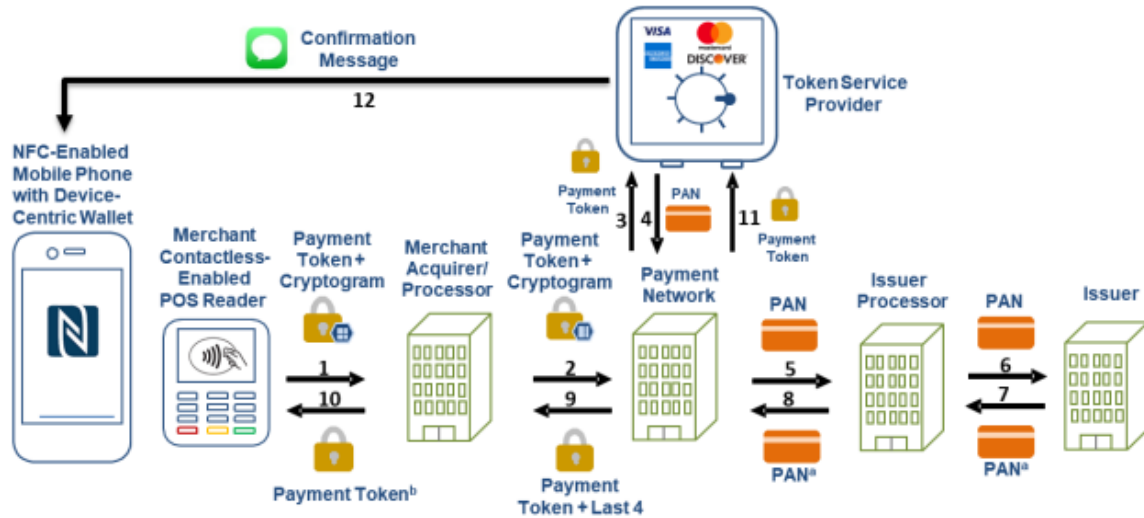
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

24. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a Texas Capital account holder requests Texas Capital to provision a specific Texas Capital debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Texas Capital card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the

request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

25. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Texas Capital card account holders for provisioning a specific Texas Capital debit and/or credit card for use on their mobile devices. The messaging gateway is also programmed to receive requests initiated by Texas Capital card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Texas Capital card account of the account holder. This messaging gateway is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to receive the messages.

26. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to determine a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the messaging

gateway and in secure communication therewith is an authorization server that processes the received request to identify the token value sent for the account selected to be charged that was passed from the authorized user to the merchant terminal via the NFC communication link. From the token value, the server can look up the debit and/or credit card account number. The authorization server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to provide the authentication services.

27. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive within the payment authorization request transaction specific information that was input into the request by the merchant. The interface is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to provide the authentication services.

28. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

29. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

30. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

31. Defendants thus infringe one or more of the claims of the 079 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 079 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 079 Patent.

32. Texas Capital has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(a), by making, using, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

33. Texas Capital has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 079 Patent by others and Texas Capital will continue to do so unless enjoined by this Court. Texas Capital's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses,

distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 079 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Texas Capital knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 079 Patent.

34. Texas Capital continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 079 Patent.

35. Texas Capital has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 079 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

36. Texas Capital has committed these acts of infringement without license or authorization.

37. By engaging in the conduct described herein, Texas Capital has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Texas Capital is thus liable to Textile for infringement of the 079 Patent, pursuant to 35 U.S.C. § 271.

38. As a direct and proximate result of Texas Capital's infringement of the 079 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Texas Capital's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

39. In addition, the infringing acts and practices of Texas Capital have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Texas Capital is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Texas Capital is finally and permanently enjoined from further infringement.

40. Texas Capital has had actual knowledge of the 079 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Texas Capital will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 079 Patent.

41. Texas Capital has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 079 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

42. Textile has been damaged as a result of the infringing conduct by Texas Capital alleged above. Thus, Texas Capital is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

43. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 079 Patent.

COUNT II

INFRINGEMENT OF U.S. PATENT NO. 8,533,802

44. On September 10, 2013, United States Patent No. 8,533,802 (“the 802 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

45. Textile is the owner of the 802 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 802 Patent against infringers, and to collect damages for all relevant times.

46. Texas Capital offers debit and/or credit cards, such as the Texas Capital Visa Debit Cards, that are used with an authentication system that authenticates the identity of a Texas Capital card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Texas Capital card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated

by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.

Debit Card Solutions

All Texas Capital Bank checking accounts come with a Visa® Debit Card with embedded chip technology as well as magnetic stripe functionality. Features include:

Enjoy an easier way of paying in stores or within apps with [Apple Pay](#)®, [Samsung Pay](#)®, and [Google Pay](#)®

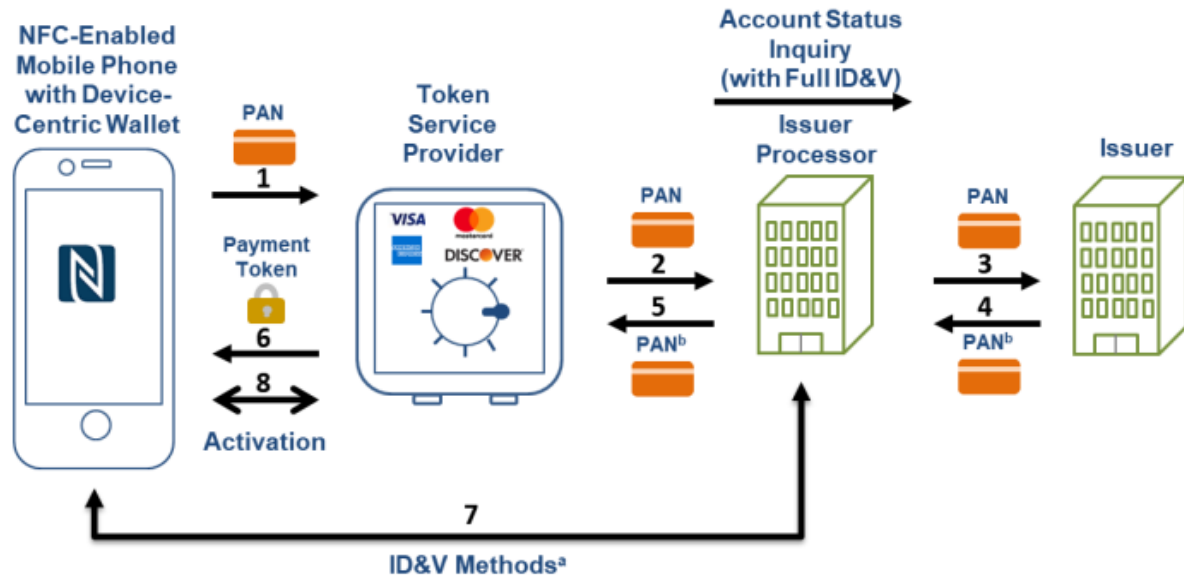
Fraud Protection: We rely on the latest technology and strategies to protect your account from fraud:

- **CardValet:** Manage your debit card usage through your mobile device by defining when, where and how your payment card is used with CardValet. [Learn more about CardValet.](#)
- **Chip Technology:** When your card is used at a chip card reader, each transaction generates a unique, one-time code, providing an added layer of security.
- **Limits:** For added protection, your card provides a daily \$4,000 point of sale limit, along with a daily ATM limit of \$500.
- **Real-Time Fraud Monitoring:** When debit card transactions fall out of your normal spending patterns, we'll contact you to make sure the transaction is actually yours.
- **Visa® Zero Liability Protection:** With [Visa Secure](#), you're not liable for any unauthorized debit card transactions when you notify the bank promptly.

(Source: <https://www.texascapitalbank.com/personal-banking/debit-credit-card-services>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

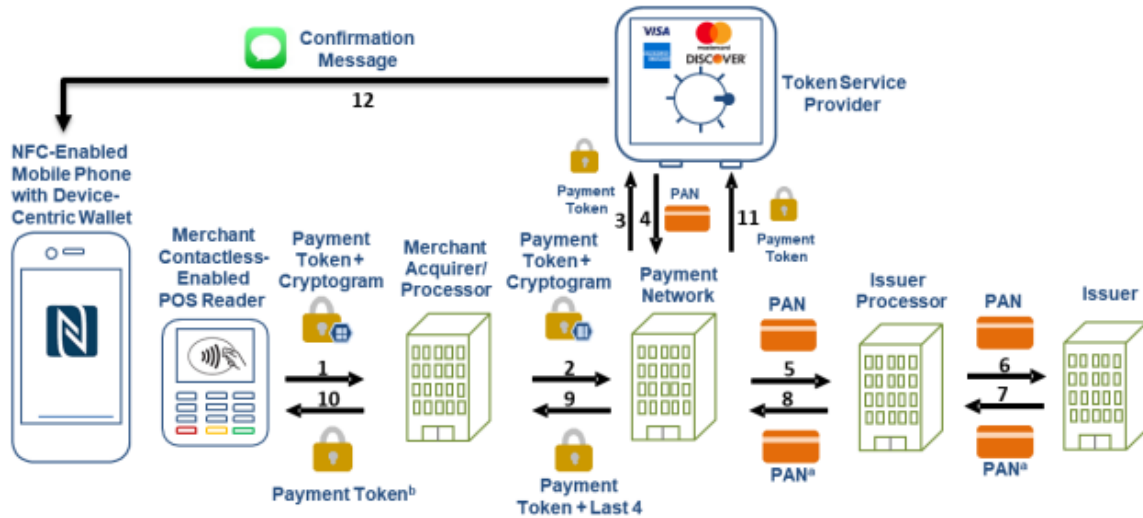
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

47. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a Texas Capital account holder requests Texas Capital to provision a specific Texas Capital debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Texas Capital card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the

request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

48. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Texas Capital card account holders for provisioning a specific Texas Capital debit and/or credit card for use on their mobile devices. This messaging gateway is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to receive the messages.

49. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate a key string adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the message gateway and in secure communication therewith is an authorization server that generates a token corresponding to the debit and/or credit card account number. The authorization server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to provide the authentication services.

50. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive transaction specific information that was input into the request by the merchant, *e.g.*, the merchant ID, invoice number, invoice amount, and date/timestamp. The interface is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to provide the authentication services.

51. The Accused Instrumentality includes a first set of instructions further operable to communicate the key string to the authorized user that the requester purports to be. For example, the messaging gateway sends the generated token to the authorized user's mobile device for use in merchant transactions.

52. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

53. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

54. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

55. Defendants thus infringe one or more claims of the 802 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 802 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 802 Patents.

56. Texas Capital has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

57. Texas Capital has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 802 Patent by others and Texas Capital will continue to do so unless enjoined by this Court. Texas Capital's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing

the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 802 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Texas Capital knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 802 Patent.

58. Texas Capital continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 802 Patent.

59. Texas Capital has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 802 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

60. Texas Capital has committed these acts of infringement without license or authorization.

61. By engaging in the conduct described herein, Texas Capital has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Texas Capital is thus liable to Textile for infringement of the 802 Patent, pursuant to 35 U.S.C. § 271.

62. As a direct and proximate result of Texas Capital's infringement of the 802 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Texas Capital's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

63. In addition, the infringing acts and practices of Texas Capital have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Texas Capital is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Texas Capital is finally and permanently enjoined from further infringement.

64. Texas Capital has had actual knowledge of the 802 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Texas Capital will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 802 Patent.

65. Texas Capital has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 802 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

66. Textile has been damaged as a result of the infringing conduct by Texas Capital alleged above. Thus, Texas Capital is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

67. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 802 Patent.

COUNT III

INFRINGEMENT OF U.S. PATENT NO. 9,584,499

68. On February 28, 2017, United States Patent No. 9,584,499 (“the 499 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

69. Textile is the owner of the 499 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 499 Patent against infringers, and to collect damages for all relevant times.

70. Texas Capital offers debit and/or credit cards, such as the Texas Capital Visa Debit Cards, that are used by Texas Capital in practicing a method for authorizing transaction specific access to a secured resource having a secured resource identity (the “Accused Instrumentality”). The Texas Capital transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The

requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.

Debit Card Solutions

All Texas Capital Bank checking accounts come with a Visa® Debit Card with embedded chip technology as well as magnetic stripe functionality. Features include:

Enjoy an easier way of paying in stores or within apps with [Apple Pay](#)®, [Samsung Pay](#)®, and [Google Pay](#)®

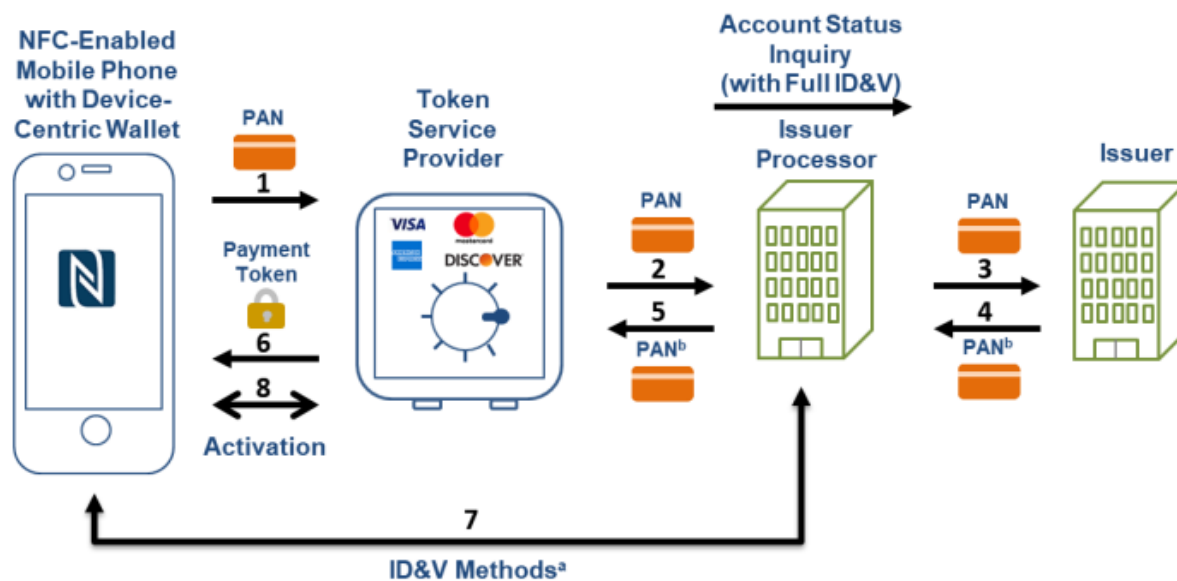
Fraud Protection: We rely on the latest technology and strategies to protect your account from fraud:

- **CardValet:** Manage your debit card usage through your mobile device by defining when, where and how your payment card is used with CardValet. [Learn more about CardValet.](#)
- **Chip Technology:** When your card is used at a chip card reader, each transaction generates a unique, one-time code, providing an added layer of security.
- **Limits:** For added protection, your card provides a daily \$4,000 point of sale limit, along with a daily ATM limit of \$500.
- **Real-Time Fraud Monitoring:** When debit card transactions fall out of your normal spending patterns, we'll contact you to make sure the transaction is actually yours.
- **Visa® Zero Liability Protection:** With [Visa Secure](#), you're not liable for any unauthorized debit card transactions when you notify the bank promptly.

(Source: <https://www.texascapitalbank.com/personal-banking/debit-credit-card-services>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

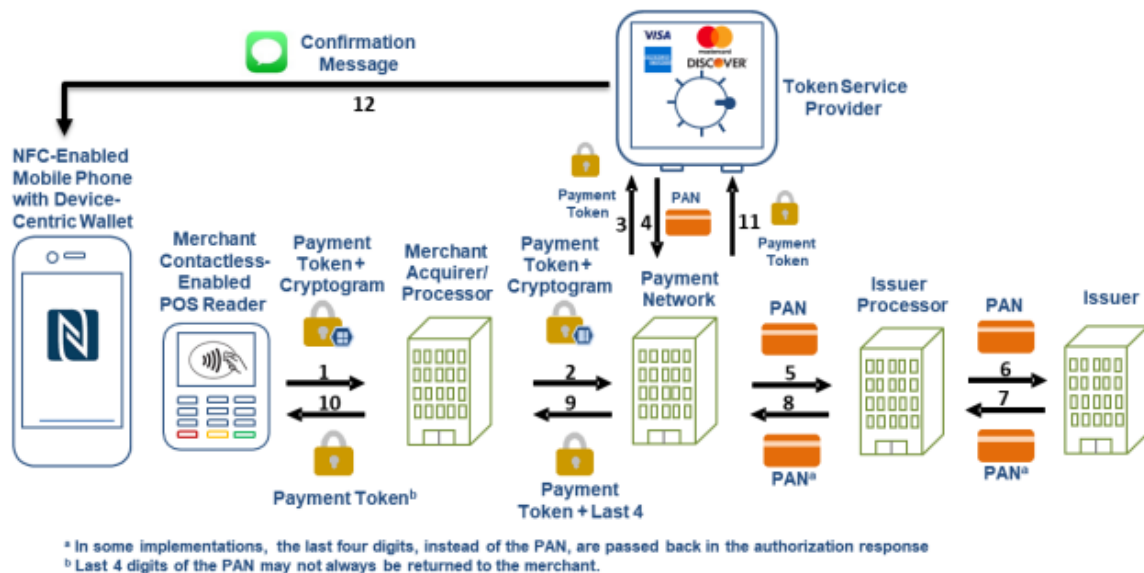


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

71. Texas Capital's use of the Accused Instrumentality includes a method for authorizing transaction specific access to a secured resource having a secured resource identity. For example, a Texas Capital account holder requests Texas Capital to provision a specific Texas Capital debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Texas Capital card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the

request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram.

72. The Accused Instrumentality includes receiving at a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive a request for transaction specific access to a secured resource by a service client. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Texas Capital card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Texas Capital card account of the account holder. This messaging gateway is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to receive the messages.

73. The Accused Instrumentality includes generating a key string with a server in communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate the key string known to both said server and an authorized user of the secured resource, said key string being associated with the secured resource within a key string table accessible by the server and providing a basis for authenticating the secured resource identity by searching the key string table for the key string. For example, behind the firewall of the messaging gateway and in communication therewith is

an authorization server that generates a token corresponding to a secured resource during the provisioning process. After this, the authorization server updates a table that maps token numbers to secured resource identities. The authorization server is then able to search the table to authenticate a secured resource identity by searching the table for the token. If the token has a corresponding secured resource identity, that identity is authenticated. The authorization server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to provide the authentication services.

74. The Accused Instrumentality includes determining transaction specific information with the server in communication with the messaging gateway, the server having a third set of instructions embodied in a computer readable medium operable to identify transaction specific information within the request. For example, the authorization server is also programmed to identify within the payment authorization request transaction specific information that was passed by the merchant. The authorization server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to provide the authentication services.

75. The Accused Instrumentality includes communicating said key string to said authorized user. For example, once the provisioning process is complete, the messaging gateway and/or the server send the token to the authorized user's mobile device. The messaging gateway is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to provide the authentication services. The authorization server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to provide the authentication services.

76. The Accused Instrumentality includes receiving an authentication credential from said service client, said authentication credential having been provided to said service client by said authorized user. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant. The authorization server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to provide the authentication services.

77. The Accused Instrumentality includes evaluating said authentication credential. For example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authorizes the transaction specific access. The authorization server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to provide the authentication services.

78. The Accused Instrumentality includes wherein the key string and authentication credential do not reveal any primary identifier associated with said secured resource. For example, neither the token nor the cryptogram reveals the debit and/or credit card number associated with the secured resource.

79. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

80. Defendants thus infringe one or more claims of the 499 Patent. The elements and conduct described herein are covered by and infringe upon at least Claim 3 of the 499 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 499 Patent.

81. Texas Capital has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

82. Texas Capital has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 499 Patent by others and Texas Capital will continue to do so unless enjoined by this Court. Texas Capital's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 499 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Texas Capital knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 499 Patent.

83. Texas Capital continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 499 Patent.

84. Texas Capital has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 499 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

85. Texas Capital has committed these acts of infringement without license or authorization.

86. By engaging in the conduct described herein, Texas Capital has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Texas Capital is thus liable to Textile for infringement of the 499 Patent, pursuant to 35 U.S.C. § 271.

87. As a direct and proximate result of Texas Capital's infringement of the 499 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Texas Capital's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

88. In addition, the infringing acts and practices of Texas Capital have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Texas Capital is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Texas Capital is finally and permanently enjoined from further infringement.

89. Texas Capital has had actual knowledge of the 499 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Texas Capital will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 499 Patent.

90. Texas Capital has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 499 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

91. Textile has been damaged as a result of the infringing conduct by Texas Capital alleged above. Thus, Texas Capital is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

92. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 499 Patent.

COUNT IV

INFRINGEMENT OF U.S. PATENT NO. 10,148,659

93. On December 4, 2018, United States Patent No. 10,148,659 (“the 659 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

94. Textile is the owner of the 659 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 659 Patent against infringers, and to collect damages for all relevant times.

95. Texas Capital offers debit and/or credit cards, such as the Texas Capital Visa Debit Cards, that are used with a computer-implemented system for a credit or debit and/or credit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit and/or credit card account number to the merchant (the “Accused Instrumentality”). The Texas Capital transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.

Debit Card Solutions

All Texas Capital Bank checking accounts come with a Visa® Debit Card with embedded chip technology as well as magnetic stripe functionality. Features include:

Enjoy an easier way of paying in stores or within apps with [Apple Pay](#)®, [Samsung Pay](#)®, and [Google Pay](#)®.

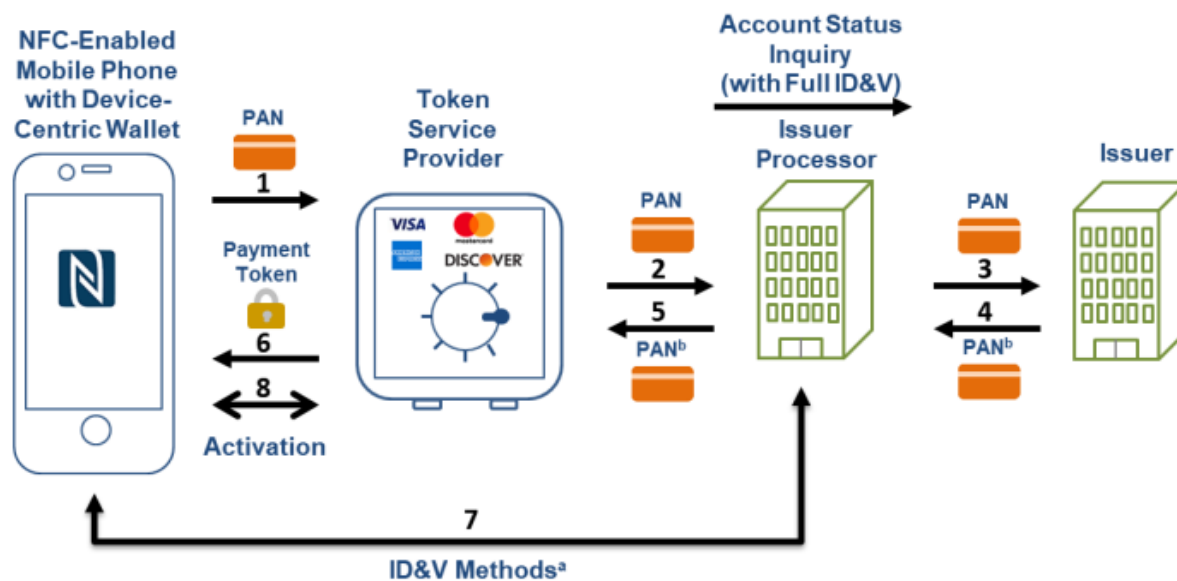
Fraud Protection: We rely on the latest technology and strategies to protect your account from fraud:

- **CardValet:** Manage your debit card usage through your mobile device by defining when, where and how your payment card is used with CardValet. [Learn more about CardValet.](#)
- **Chip Technology:** When your card is used at a chip card reader, each transaction generates a unique, one-time code, providing an added layer of security.
- **Limits:** For added protection, your card provides a daily \$4,000 point of sale limit, along with a daily ATM limit of \$500.
- **Real-Time Fraud Monitoring:** When debit card transactions fall out of your normal spending patterns, we'll contact you to make sure the transaction is actually yours.
- **Visa® Zero Liability Protection:** With [Visa Secure](#), you're not liable for any unauthorized debit card transactions when you notify the bank promptly.

(Source: <https://www.texascapitalbank.com/personal-banking/debit-credit-card-services>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

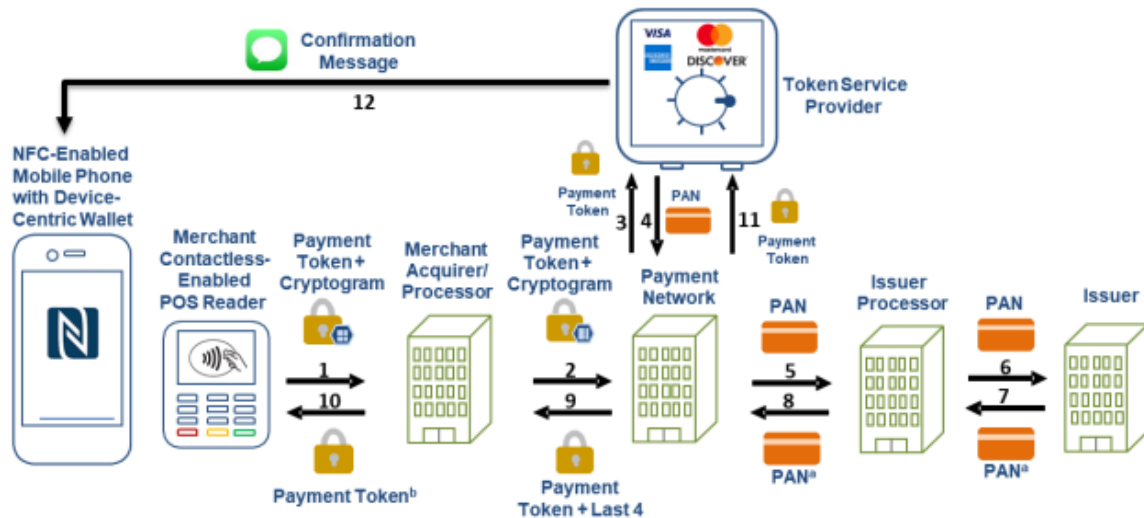
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

96. The Accused Instrumentality includes a computer-implemented system for a credit or debit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit card account number to the merchant. For example, a Texas Capital account holder requests Texas Capital to provision a specific Texas Capital debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Texas Capital to a specific merchant in a specific amount for a specific transaction from

a specific Texas Capital card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

97. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a credit or debit card account holder's mobile device, a merchant's payment application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a Texas Capital card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Texas Capital card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Texas Capital card account of the account holder. This interface is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to receive the messages.

98. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration

information received from the credit or debit card account holder through the at least one interface, the registration information comprising a credit or debit card account holder identifier and at least one credit or debit card account number having an associated unique account identifier wherein the credit or debit card account number and unique account identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card and the debit and/or credit card account number (which has a corresponding token), received from Texas Capital card account holders through the interface for provisioning a specific Texas Capital debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Texas Capital card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Texas Capital card account of the account holder. The server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to receive the messages.

99. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to pay the specific merchant for the specific transaction from a given debit or credit card account, the authorization request message having been received through the at least one interface and originating from the credit or debit card account holder's mobile device and comprising: a first merchant identifier; a first transaction specific information selected from the group consisting of a first transaction amount and first client reference identifier; the credit or debit card account holder identifier; and a designated unique account identifier selected from the at least one unique account identifiers. For example, the Accused

Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Texas Capital card account holder's mobile device. The server is programmed to receive authorization requests initiated by Texas Capital card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a merchant identifier, and the Texas Capital card account holder identifier. The server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to receive the messages.

100. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string wherein the key string is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the designated unique account identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to receive the messages.

101. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive a payment request message from the merchant's payment application through the at least one interface, the payment request message comprising: a second merchant identifier; a second transaction specific information selected from the group consisting of a second transaction amount and second client reference identifier; and a second transaction specific authentication credential whereby the second authentication credential was received by the merchant application from the credit or debit card account holder's mobile device. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Texas Capital card account holder's mobile device. The server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to receive the messages.

102. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the credit or debit card account holder's request to use the credit or debit card account number associated with the designated unique account identifier for payment to the specific merchant for the specific transaction and authorizing the resource provider to use the credit or debit card account number associated with the designated unique account identifier to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or bank account number to the

specific merchant by determining if: the first merchant identifier matches the second merchant identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to provide the authentication services.

103. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

104. Defendants thus infringe one or more claims of the 659 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 9 of the 659 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 659 Patent.

105. Texas Capital has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35

U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

106. Texas Capital has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 659 Patent by others and Texas Capital will continue to do so unless enjoined by this Court. Texas Capital's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 659 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Texas Capital knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 659 Patent.

107. Texas Capital continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 659 Patent.

108. Texas Capital has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 9 of the 659 Patent, in violation of 35 U.S.C.

§ 271(c), by contributing to the direct infringement of the 659 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

109. Texas Capital has committed these acts of infringement without license or authorization.

110. By engaging in the conduct described herein, Texas Capital has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Texas Capital is thus liable to Textile for infringement of the 659 Patent, pursuant to 35 U.S.C. § 271.

111. As a direct and proximate result of Texas Capital's infringement of the 659 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Texas Capital's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

112. In addition, the infringing acts and practices of Texas Capital have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Texas Capital is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Texas Capital is finally and permanently enjoined from further infringement.

113. Texas Capital has had actual knowledge of the 659 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Texas Capital will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 659 Patent.

114. Texas Capital has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 659 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

115. Textile has been damaged as a result of the infringing conduct by Texas Capital alleged above. Thus, Texas Capital is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

116. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 659 Patent.

COUNT V

INFRINGEMENT OF U.S. PATENT NO. 10,560,454

117. On February 11, 2020, United States Patent No. 10,560,454 (“the 454 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

118. Textile is the owner of the 454 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 454 Patent against infringers, and to collect damages for all relevant times.

119. Texas Capital offers debit and/or credit cards, such as the Texas Capital Visa Debit Cards, that are used with a computer-implemented system for a user to authorize a

resource authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client (the "Accused Instrumentality"). The Texas Capital transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.

Debit Card Solutions

All Texas Capital Bank checking accounts come with a Visa® Debit Card with embedded chip technology as well as magnetic stripe functionality. Features include:

Enjoy an easier way of paying in stores or within apps with [Apple Pay](#)¹, [Samsung Pay](#)², and [Google Pay](#)³

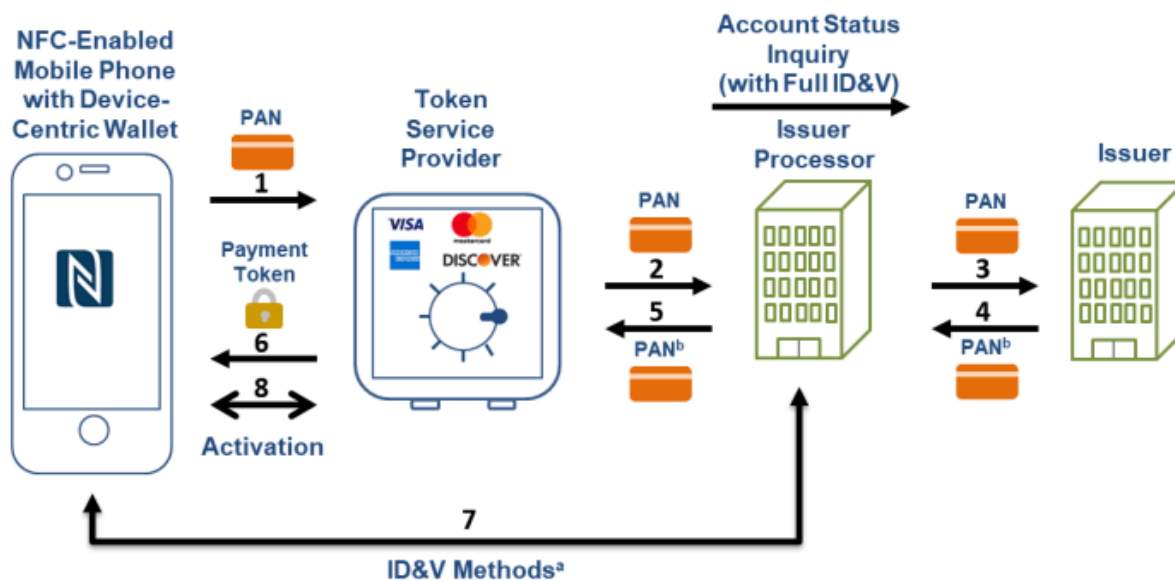
Fraud Protection: We rely on the latest technology and strategies to protect your account from fraud:

- **CardValet:** Manage your debit card usage through your mobile device by defining when, where and how your payment card is used with CardValet. [Learn more about CardValet.](#)
- **Chip Technology:** When your card is used at a chip card reader, each transaction generates a unique, one-time code, providing an added layer of security.
- **Limits:** For added protection, your card provides a daily \$4,000 point of sale limit, along with a daily ATM limit of \$500.
- **Real-Time Fraud Monitoring:** When debit card transactions fall out of your normal spending patterns, we'll contact you to make sure the transaction is actually yours.
- **Visa® Zero Liability Protection:** With [Visa Secure](#), you're not liable for any unauthorized debit card transactions when you notify the bank promptly.

(Source: <https://www.texascapitalbank.com/personal-banking/debit-credit-card-services>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

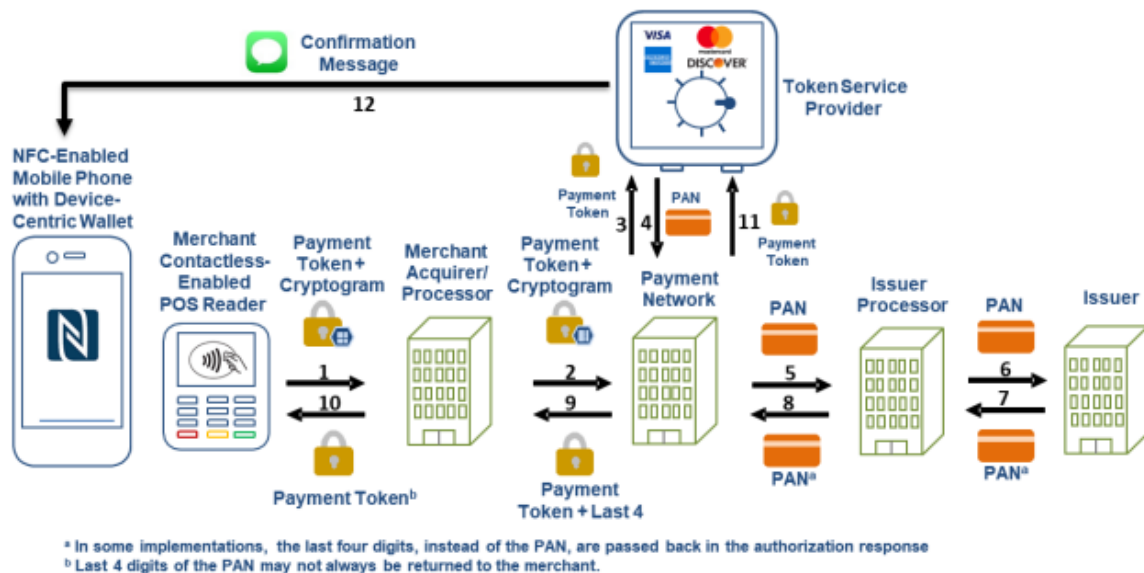


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

120. The Accused Instrumentality includes a computer-implemented system for a user to authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client. For example, a Texas Capital account holder requests Texas Capital to provision a specific Texas Capital debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Texas Capital to a specific merchant in a specific amount for a specific transaction from a specific Texas Capital card account of the

account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

121. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a user's application, a service client's application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a Texas Capital card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Texas Capital card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Texas Capital card account of the account holder. This interface is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to receive the messages.

122. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration

information received from the user through the at least one interface, the registration information comprising a user identifier and at least one secured resource identifier associated with the common identifier of the secured resource, wherein the common identifier and secured resource identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card, the debit and/or credit card account number (which has a corresponding token), and the CVV number received from Texas Capital card account holders through the interface for provisioning a specific Texas Capital debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Texas Capital card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Texas Capital card account of the account holder. The server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to receive the messages.

123. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to authorize access to the secured resource by the service client, the authorization request message having been received through the at least one interface from the user's application and comprising: a first service client identifier; a first transaction specific information; the user identifier; and a designated secured resource identifier selected from one of the at least one secured resource identifiers. For example, the Accused Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Texas Capital

card account holder's mobile device. The server is programmed to receive authorization requests initiated by Texas Capital card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a CVV number, a merchant identifier, other token information, and the Texas Capital card account holder identifier. The server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to receive the messages.

124. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string and does not include or reveal the common identifier associated with the designated secured resource identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to receive the messages.

125. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive an access request message from the service client's application through the at least one interface, the

payment request message comprising: a second service client identifier; a second transaction specific information; and a second transaction specific authentication credential whereby the second transaction specific authentication credential was received by the service client's application from the user's application. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Texas Capital card account holder's mobile device. The server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to receive the messages.

126. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the user's request to access the secured resource associated with the designated secured resource identifier without transmitting or otherwise providing the common identifier of the secured resource to the service client by determining if: the first service client identifier matches the second service client identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of

requestor as the actual account holder. The server is either hosted directly by Texas Capital or through an agent with whom Texas Capital has contracted to provide the authentication services.

127. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

128. Defendants thus infringe one or more claims of the 454 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 8 of the 454 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 454 Patent.

129. Texas Capital has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

130. Texas Capital has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 454 Patent by others and Texas Capital will continue to do so unless enjoined by this Court. Texas Capital's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing

the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 454 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Texas Capital knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 454 Patent.

131. Texas Capital continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 454 Patent.

132. Texas Capital has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 454 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

133. Texas Capital has committed these acts of infringement without license or authorization.

134. By engaging in the conduct described herein, Texas Capital has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Texas Capital is thus liable to Textile for infringement of the 454 Patent, pursuant to 35 U.S.C. § 271.

135. As a direct and proximate result of Texas Capital's infringement of the 454 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Texas Capital's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

136. In addition, the infringing acts and practices of Texas Capital have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Texas Capital is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Texas Capital is finally and permanently enjoined from further infringement.

137. Texas Capital has had actual knowledge of the 454 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Texas Capital will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 454 Patent.

138. Texas Capital has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 454 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

139. Textile has been damaged as a result of the infringing conduct by Texas Capital alleged above. Thus, Texas Capital is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

140. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 454 Patent.

ADDITIONAL ALLEGATIONS REGARDING INFRINGEMENT

141. Texas Capital has also indirectly infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by inducing others to directly infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Texas Capital has induced the end-users, Texas Capital's customers, to directly infringe (literally and/or under the doctrine of equivalents) the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by using the Accused Instrumentality.

142. Texas Capital took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

143. Such steps by Texas Capital included, among other things, advising or directing customers and end-users to use the Accused Instrumentality in an infringing manner; advertising and promoting the use of the Accused Instrumentality in an infringing manner; and/or distributing instructions that guide users to use the Accused Instrumentality in an infringing manner.

144. Texas Capital has performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts constitute infringement, at least since the filing of the Complaint.

145. Texas Capital was and is aware that the normal and customary use of the Accused Instrumentality by Texas Capital's customers would infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Texas Capital's inducement is ongoing.

146. Texas Capital directs or controls the use of the Accused Instrumentality nationwide through its own websites and in its own branches, including in Texas and elsewhere in the United States, and expects and intends that the Accused Instrumentality will be so used.

147. Texas Capital took active steps, directly and/or through contractual relationships with others, with the specific intent to cause such persons to make or use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

148. Texas Capital performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts would constitute infringement.

149. Texas Capital's inducement is ongoing.

150. Texas Capital has also indirectly infringed by contributing to the infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Texas Capital has contributed to the direct infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by the end-user of the Accused Instrumentality.

151. The Accused Instrumentality has special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

152. As described above, the special features include securely authorizing specific transactions without providing a credit or debit card number to the merchant used in a manner that infringes the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

153. The special features constitute a material part of the invention of one or more of the claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and are not staple articles of commerce suitable for substantial non-infringing use.

154. Texas Capital's contributory infringement is ongoing.

155. Texas Capital's actions are at least objectively reckless as to the risk of infringing valid patents and this objective risk was either known or should have been known by Texas Capital, at least since the filing of the Complaint.

156. Texas Capital has had knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent at least since the filing of the Complaint.

157. Texas Capital's customers have infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

158. Texas Capital encouraged its customers' infringement.

159. Texas Capital's direct and indirect infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent is, has been, and/or continues to be willful, intentional, deliberate, and/or in conscious disregard of Textile's rights under the patents.

160. Textile has been damaged as a result of the infringing conduct by Texas Capital alleged above. Thus, Texas Capital is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Textile hereby requests a trial by jury on all issues so triable by right.

PRAYER FOR RELIEF

Textile requests that the Court find in its favor and against Texas Capital, and that the Court grant Textile the following relief:

- a. Judgment that one or more claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent have been infringed, either literally and/or under the doctrine of equivalents, by Texas Capital and/or all others acting in concert therewith;
- b. A permanent injunction enjoining Texas Capital and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert therewith from infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent; or, in the alternative, an award of a reasonable ongoing royalty for future infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by such entities;
- c. Judgment that Texas Capital account for and pay to Textile all damages to and costs incurred by Textile because of Texas Capital's infringing activities and other conduct complained of herein, including an award of all increased damages to which Textile is entitled under 35 U.S.C. § 284;
- d. That Textile be granted pre-judgment and post-judgment interest on the damages

caused by Texas Capital's infringing activities and other conduct complained of herein;

e. That this Court declare this an exceptional case and award Textile its reasonable attorney's fees and costs in accordance with 35 U.S.C. § 285; and

f. That Textile be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: October 12, 2021

Respectfully submitted,

/s/ Matthew J. Antonelli

Matthew J. Antonelli

Texas Bar No. 24068432

matt@ahtlawfirm.com

Zachariah S. Harrington

Texas Bar No. 24057886

zac@ahtlawfirm.com

Larry D. Thompson, Jr.

Texas Bar No. 24051428

larry@ahtlawfirm.com

Christopher Ryan Pinckney

Texas Bar No. 24067819

ryan@ahtlawfirm.com

ANTONELLI, HARRINGTON

& THOMPSON LLP

4306 Yoakum Blvd., Ste. 450

Houston, TX 77006

(713) 581-3000

Stafford Davis

State Bar No. 24054605

sdavis@stafforddavisfirm.com

Catherine Bartles

Texas Bar No. 24104849

cbartles@stafforddavisfirm.com

THE STAFFORD DAVIS FIRM

815 South Broadway Avenue

Tyler, Texas 75701

(903) 593-7000

(903) 705-7369 fax

Of Counsel:

Sandeep Seth

Texas State Bar No. 18043000
SETHLAW
Pennzoil Place
700 Milam Street, Suite 1300
Houston, Texas 77002
Telephone: (713) 244-5017
ss@sethlaw.com

Attorneys for Textile Computer Systems, Inc.

EXHIBIT 2H

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

TEXTILE COMPUTER SYSTEMS, INC.,

Plaintiff,

v.

VANTAGE BANK TEXAS,

Defendant.

CIVIL ACTION NO. 6:21-cv-1058

ORIGINAL COMPLAINT FOR
PATENT INFRINGEMENT

JURY TRIAL DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Textile Computer Systems, Inc. (“Textile” or “Plaintiff”) files this original complaint against Defendant Vantage Bank Texas (“Vantage”), alleging, based on its own knowledge as to itself and its own actions and based on information and belief as to all other matters, as follows:

PARTIES

1. Textile Computer Systems, Inc. is a corporation formed under the laws of the State of Texas, with a place of business at 618 Bluff Trail, San Antonio, Texas, 78216.

2. Vantage Bank Texas is a bank organized and existing under the laws of Texas. Vantage Bank Texas has its headquarters at 45 Northeast Loop 410, Suite 500, San Antonio, Texas 78216.

3. Vantage and its affiliates lead and are part of an interrelated group of companies which together comprise one of the country’s largest banking and financial service entities, including under the Vantage brand.

4. Vantage and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

5. Vantage and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

6. Vantage and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

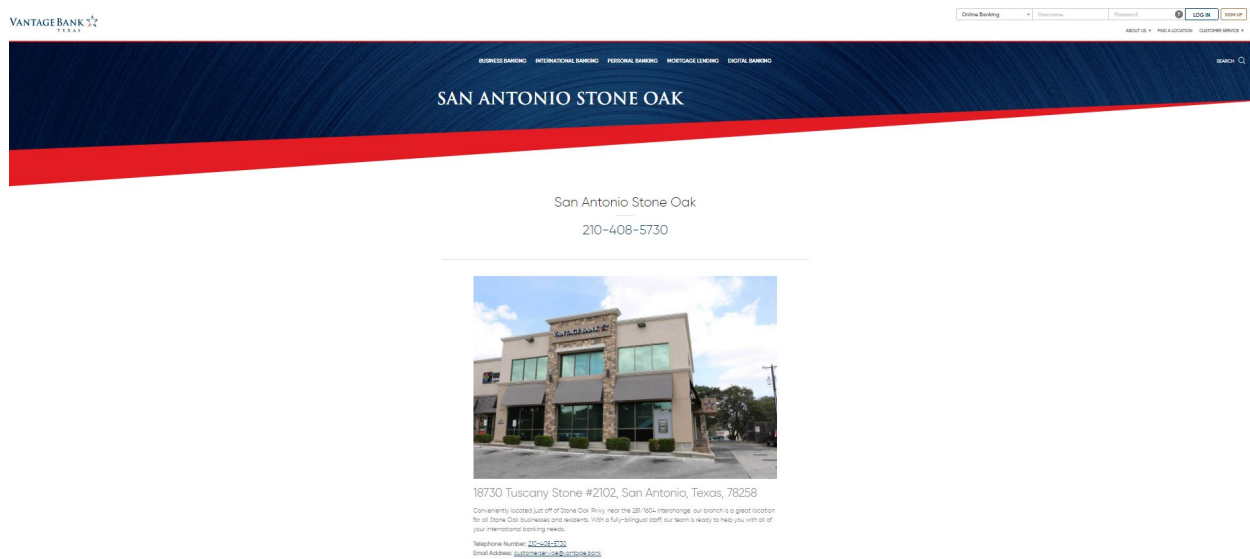
7. Thus, Vantage and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

JURISDICTION AND VENUE

8. This is an action for infringement of United States patents arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. § 1331 and § 1338(a).

9. This Court has personal jurisdiction over Vantage pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Vantage has done and continues to do business in Texas; and (ii) Vantage has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations, inducing others to commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein.

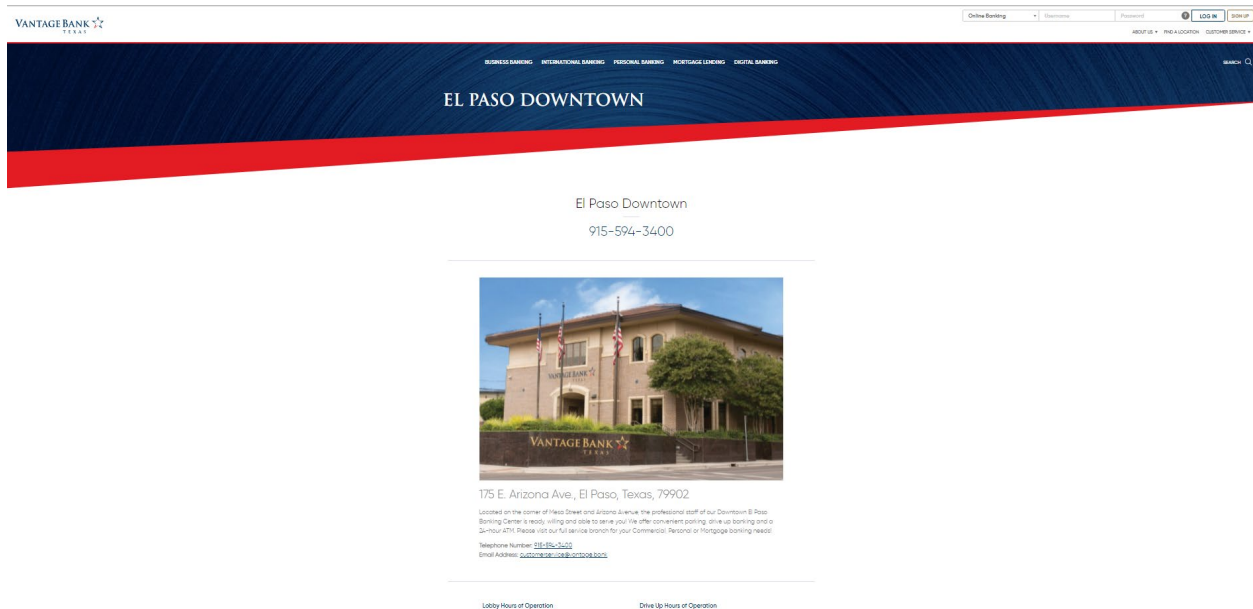
10. Venue is proper in this district pursuant to 28 U.S.C. § 1400(b). Venue is further proper because Vantage has committed and continues to commit acts of patent infringement in this district. For example, Vantage cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those cardholders make and/or use the accused instrumentalities in the district. Vantage induces others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. Vantage has regular and established places of business in this district, including at least at 18730 Tuscany Stone, Suite 2102, San Antonio, Texas 78258, at 175 E. Arizona Ave., El Paso, Texas 79902, and at numerous other locations in San Antonio and El Paso:



(Source: <https://www.vantage.bank/en/customer-service/banking-center-locations/san-antonio-stone-oak/>)



(Source: screenshot from Google Maps Street View)



(Source: <https://www.vantage.bank/en/customer-service/banking-center-locations/el-paso-downtown-banking-center/>)



(Source: screenshot from Google Maps Street View)

BACKGROUND

11. The patents-in-suit generally pertain to payment authorization technology used in payment networks used to process transactions from, for example, credit cards and debit cards. The technology disclosed by the patents was developed by Gopal Nandakumar, a Texas-based entrepreneur, software engineer, and prolific inventor with over 30 years of experience in the field of Information Management Systems.

12. In 1987, after receiving Master's Degrees from both the University of Madras, India and the Georgia Institute of Technology, Mr. Nandakumar formed Textile Computer Systems, Inc. ("Textile") for the purpose of consulting and developing software for the textile industry. In 2005, Textile began transitioning into credit card transaction systems. In 2011, Textile began to develop and market the MySingleLink suite of applications.

13. The Nandakumar patents are related to payment authorization technology. Mr. Nandakumar has been at the forefront of payment authorization, developing, disclosing, and patenting solutions for reducing fraud in credit and debit card transactions. Indeed, the

Nandakumar patents (or the applications leading to them) have been cited during patent prosecution over a hundred times, including by numerous leading companies in the payment authorization industry such as ADP, Bank of America, Google, Groupon, IBM, Mastercard, NEC, Paypal, Visa, and Wells Fargo.

THE TECHNOLOGY

14. The patents-in-suit, U.S. Patent Nos. 8,505,079, 8,533,802, 9,584,499, 10,148,659, and 10,560,454 (collectively, the “Asserted Patents”), teach systems, including payment processing systems, for securely and effectively approving and processing specific credit card and/or debit card transactions. Through the specific use of servers, messaging gateways, and/or interfaces, these systems act to reduce credit card and/or debit card fraud and misuse through their use and validation of key strings, authentication credentials, transaction specific information, and transaction specific credentials. The technology in the Asserted Patents improves the underlying functionality of existing card processing infrastructure by minimizing fraud and data theft in the face of attacks on payment systems that continue to grow in their number and sophistication.

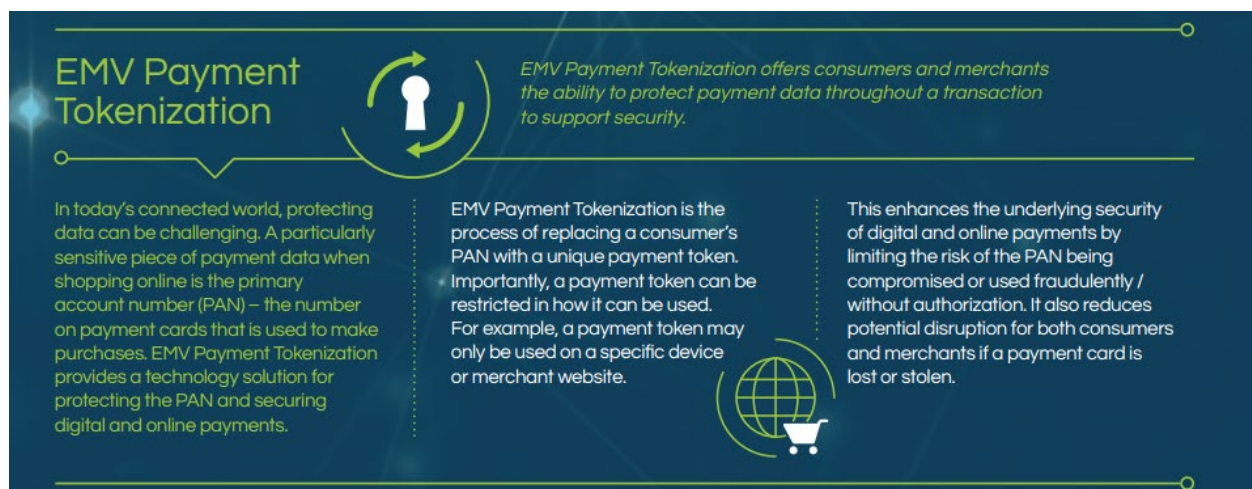
15. The patented improvements are critical for implementing secure payment systems, especially in light of the many high-profile merchant data breaches that have led to increased credit and debit card fraud. For example, in 2006, TJX Companies, who owns retailers like TJMaxx and Marshall’s, was hit with a cyber attack that resulted in the theft of credit cards leading to over \$100 million in fraud losses. In 2013, five people were indicted for attacking a number of retailers and financial institutions including NASDAQ, 7-Eleven, JCP, and others, stealing over 160 million cards. Also in 2013, the retailer Target suffered a data breach that resulted in 40 million debit and credit cards being compromised.

16. One implementation of the technology claimed in the Asserted Patents has been described by EMVCo as “a global Payment Tokenisation ecosystem that overlays and interoperates with existing payment ecosystems to support digital commerce and new methods of payment” and as “enhanc[ing] the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorized or fraudulent use of PANs.”

(Source: <https://www.emvco.com/emv-technologies/payment-tokenisation/>).

17. The technology claimed in the Asserted Patents is far from conventional technology. The payment industry gathered and consulted experts who worked together over a number of years to develop infringing payment tokenisation systems. In other words, the technology claimed in the Asserted Patents was not existing or conventional technology that the payment industry had sitting on the shelf.

18. Indeed, as recently as February of this year, EMVCo itself recognized that an implementation of the technology claimed in the Asserted Patents “provides a technology solution for protecting the PAN and securing digital and online payments”:



(Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

19. That same EMVCo document notes that “In today’s connected world, protecting data can be challenging. A particularly sensitive piece of payment data when shopping online is the primary account number (PAN) – the number on payment cards that is used to make purchases” and that EMVCo’s payment tokenization “enhances the underlying security of digital and online payments by limiting the risk of the PAN being compromised or used fraudulently / without authorization.” The document also states that the “Payment Tokenisation Specification provides an interoperable Technical Framework.” (Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

20. One of the asserted patents, the 079 Patent, was challenged in an Inter Partes Review proceeding before the Patent and Trademark Office (“PTO”). The PTO found that the challenger, Unified Patents Inc., was unable to show that one element, the “key string” as claimed in the 079 Patent claims and as construed by the PTO, was in the prior art at all, much less it being conventional or widespread. The PTO thus confirmed the patentability of all challenged claims of the 079 Patent.

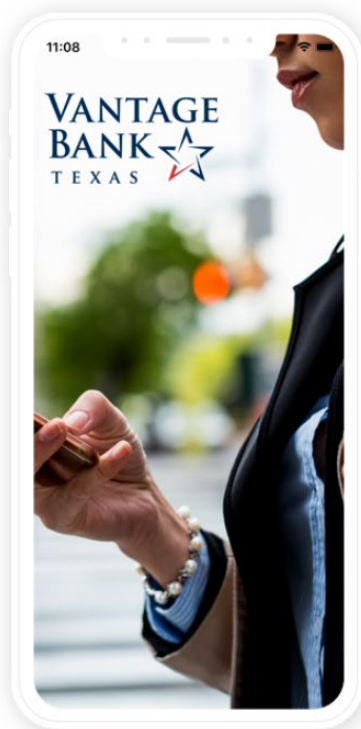
COUNT I

INFRINGEMENT OF U.S. PATENT NO. 8,505,079

21. On August 6, 2013, United States Patent No. 8,505,079 (“the 079 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

22. Textile is the owner of the 079 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 079 Patent against infringers, and to collect damages for all relevant times.

23. Vantage offers debit and/or credit cards, such as the Vantage Bank Texas Visa and Mastercard Credit Cards, that are used with an authentication system that authenticates the identity of a Vantage card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Vantage card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities, for example. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.



Detailed Features

1 DIGITAL WALLET

Your new card can make life a little easier, and help keep your financial information more secure.

[VIEW DEMO](#)

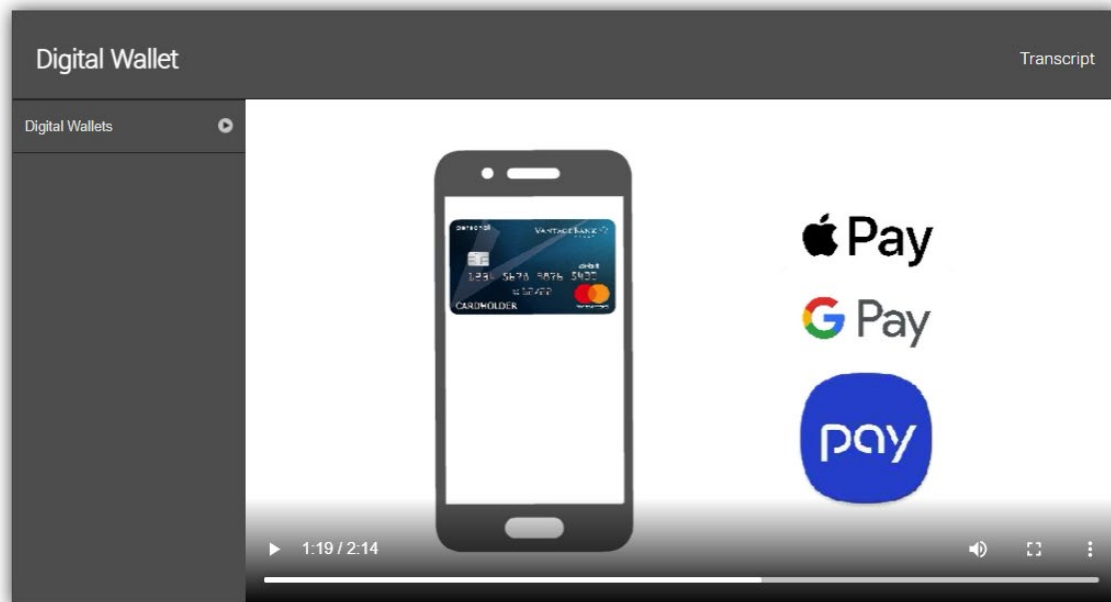
2 POPMONEY®

3 MOBILE CHECK DEPOSIT

4 CARD VALET

5 NOTIFI FOR MOBILE

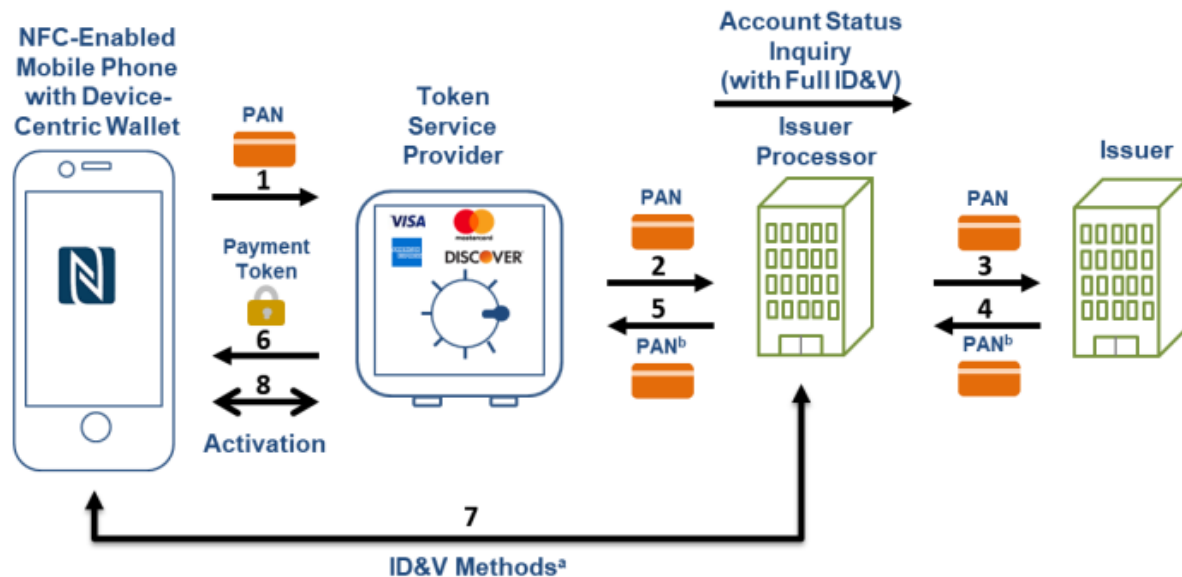
(Source: <https://www.vantage.bank/en/digital/vantage-personal-mobile/>)



(Source: <https://www.onlinebanktours.com/mobile/?b=6591&c=80164>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^a ID&V methods includes text or email or call. OTP is an example.

^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

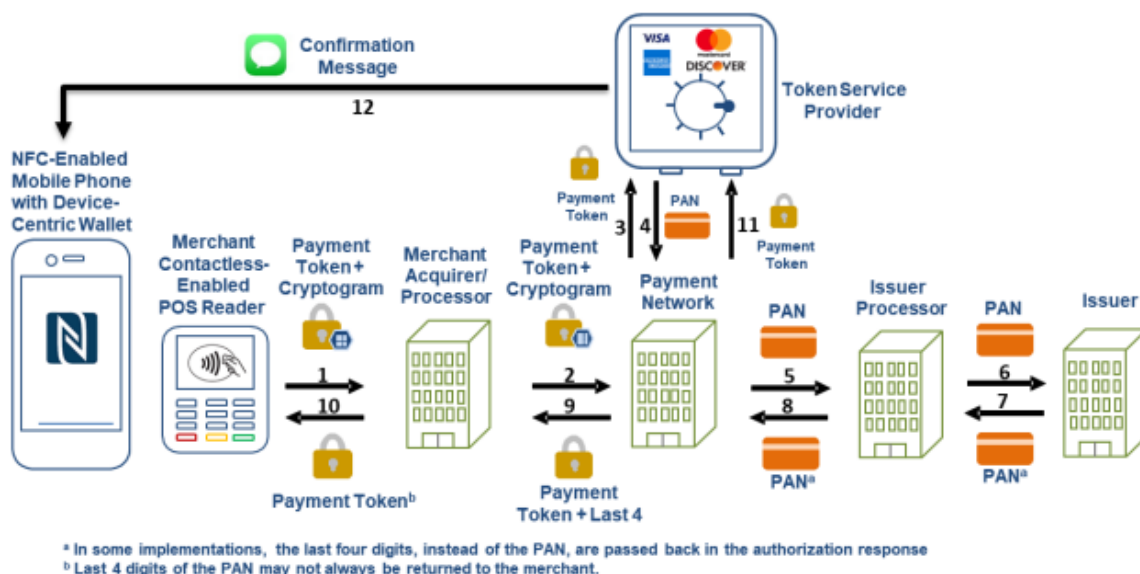


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

24. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a Vantage account holder requests Vantage to provision a specific Vantage debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Vantage card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's

smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

25. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Vantage card account holders for provisioning a specific Vantage debit and/or credit card for use on their mobile devices. The messaging gateway is also programmed to receive requests initiated by Vantage card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Vantage card account of the account holder. This messaging gateway is either hosted directly by Vantage or through an agent with whom Vantage has contracted to receive the messages.

26. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to determine a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the messaging

gateway and in secure communication therewith is an authorization server that processes the received request to identify the token value sent for the account selected to be charged that was passed from the authorized user to the merchant terminal via the NFC communication link. From the token value, the server can look up the debit and/or credit card account number. The authorization server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to provide the authentication services.

27. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive within the payment authorization request transaction specific information that was input into the request by the merchant. The interface is either hosted directly by Vantage or through an agent with whom Vantage has contracted to provide the authentication services.

28. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

29. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

30. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

31. Defendants thus infringe one or more of the claims of the 079 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 079 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 079 Patent.

32. Vantage has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(a), by making, using, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

33. Vantage has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 079 Patent by others and Vantage will continue to do so unless enjoined by this Court. Vantage's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors,

agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 079 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Vantage knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 079 Patent.

34. Vantage continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 079 Patent.

35. Vantage has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 079 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

36. Vantage has committed these acts of infringement without license or authorization.

37. By engaging in the conduct described herein, Vantage has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Vantage is thus liable to Textile for infringement of the 079 Patent, pursuant to 35 U.S.C. § 271.

38. As a direct and proximate result of Vantage's infringement of the 079 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Vantage's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

39. In addition, the infringing acts and practices of Vantage have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Vantage is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Vantage is finally and permanently enjoined from further infringement.

40. Vantage has had actual knowledge of the 079 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Vantage will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 079 Patent.

41. Vantage has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 079 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

42. Textile has been damaged as a result of the infringing conduct by Vantage alleged above. Thus, Vantage is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

43. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 079 Patent.

COUNT II

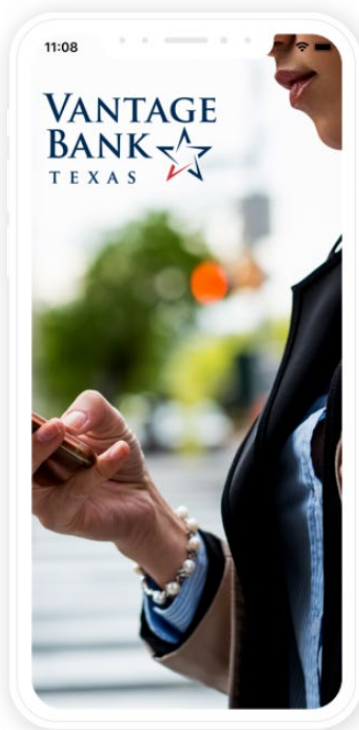
INFRINGEMENT OF U.S. PATENT NO. 8,533,802

44. On September 10, 2013, United States Patent No. 8,533,802 (“the 802 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Related Method.”

45. Textile is the owner of the 802 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 802 Patent against infringers, and to collect damages for all relevant times.

46. Vantage offers debit and/or credit cards, such as the Vantage Bank Texas Visa and Mastercard Credit Cards, that are used with an authentication system that authenticates the identity of a Vantage card holder in a request to pay a merchant for a transaction (the “Accused Instrumentality”). The Vantage card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated

by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



Detailed Features

1 DIGITAL WALLET

Your new card can make life a little easier, and help keep your financial information more secure.

[VIEW DEMO](#)

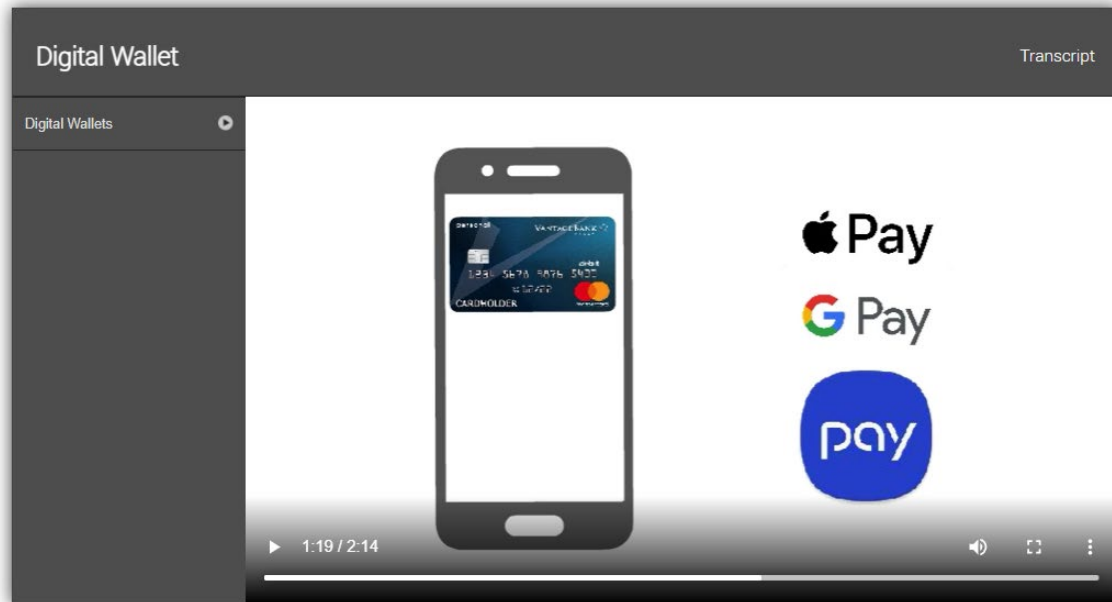
2 POPMONEY®

3 MOBILE CHECK DEPOSIT

4 CARD VALET

5 NOTIFI FOR MOBILE

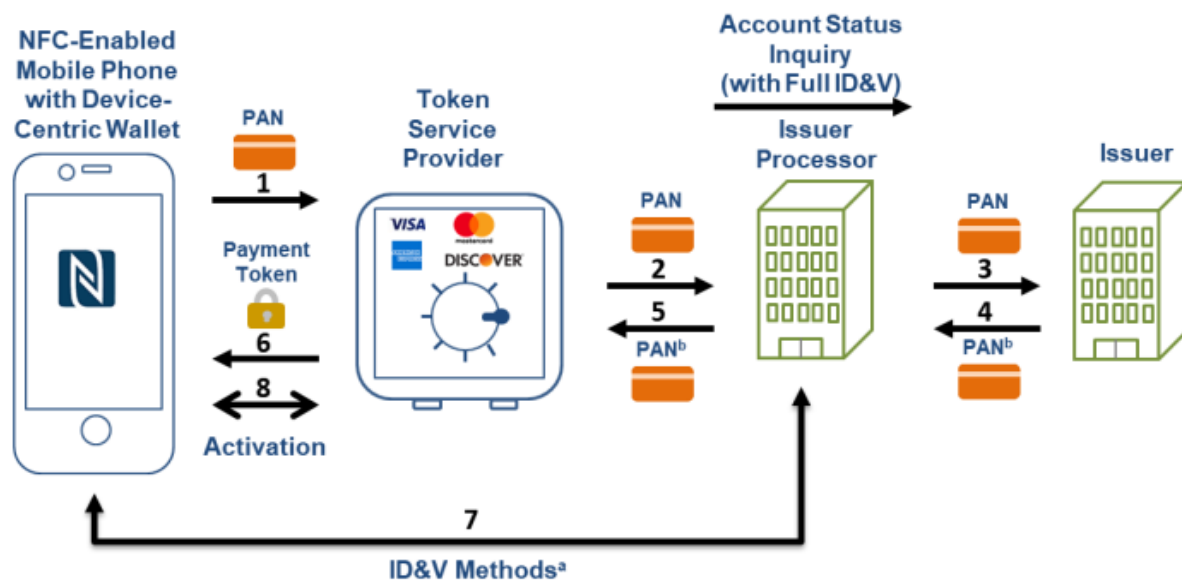
(Source: <https://www.vantage.bank/en/digital/vantage-personal-mobile/>)



(Source: <https://www.onlinebanktours.com/mobile/?b=6591&c=80164>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

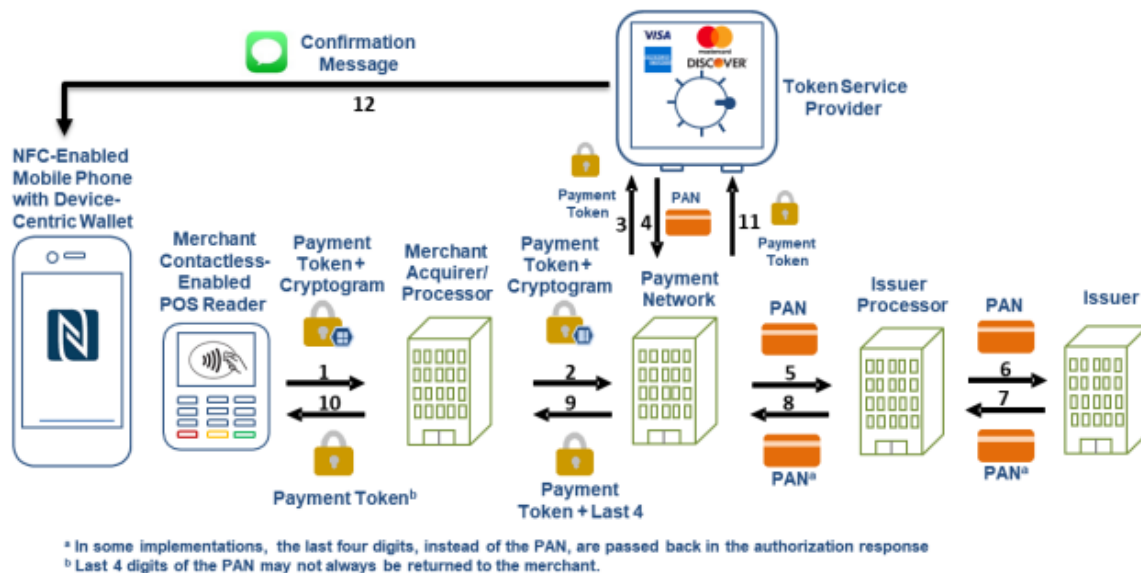


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

47. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a Vantage account holder requests Vantage to provision a specific Vantage debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Vantage card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's

smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

48. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Vantage card account holders for provisioning a specific Vantage debit and/or credit card for use on their mobile devices. This messaging gateway is either hosted directly by Vantage or through an agent with whom Vantage has contracted to receive the messages.

49. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate a key string adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the message gateway and in secure communication therewith is an authorization server that generates a token corresponding to the debit and/or credit card account number. The authorization server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to provide the authentication services.

50. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive transaction specific information that was input into the request by the merchant, *e.g.*, the merchant ID, invoice number, invoice amount, and date/timestamp. The interface is either hosted directly by Vantage or through an agent with whom Vantage has contracted to provide the authentication services.

51. The Accused Instrumentality includes a first set of instructions further operable to communicate the key string to the authorized user that the requester purports to be. For example, the messaging gateway sends the generated token to the authorized user's mobile device for use in merchant transactions.

52. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

53. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

54. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

55. Defendants thus infringe one or more claims of the 802 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 802 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 802 Patents.

56. Vantage has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

57. Vantage has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 802 Patent by others and Vantage will continue to do so unless enjoined by this Court. Vantage's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors,

agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 802 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Vantage knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 802 Patent.

58. Vantage continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 802 Patent.

59. Vantage has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 802 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

60. Vantage has committed these acts of infringement without license or authorization.

61. By engaging in the conduct described herein, Vantage has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Vantage is thus liable to Textile for infringement of the 802 Patent, pursuant to 35 U.S.C. § 271.

62. As a direct and proximate result of Vantage's infringement of the 802 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Vantage's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

63. In addition, the infringing acts and practices of Vantage have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Vantage is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Vantage is finally and permanently enjoined from further infringement.

64. Vantage has had actual knowledge of the 802 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Vantage will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 802 Patent.

65. Vantage has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 802 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

66. Textile has been damaged as a result of the infringing conduct by Vantage alleged above. Thus, Vantage is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

67. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 802 Patent.

COUNT III

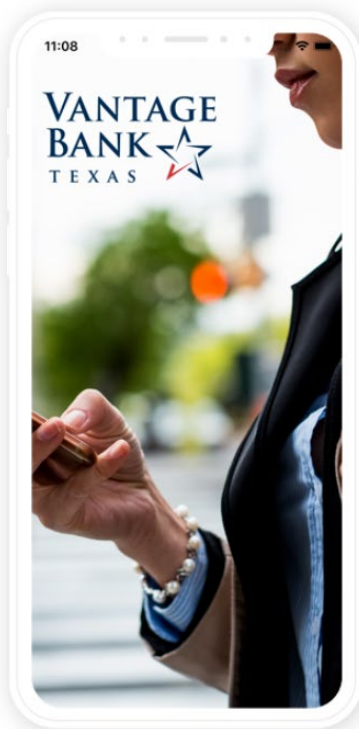
INFRINGEMENT OF U.S. PATENT NO. 9,584,499

68. On February 28, 2017, United States Patent No. 9,584,499 (“the 499 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

69. Textile is the owner of the 499 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 499 Patent against infringers, and to collect damages for all relevant times.

70. Vantage offers debit and/or credit cards, such as the Vantage Bank Texas Visa and Mastercard Credit Cards, that are used by Vantage in practicing a method for authorizing transaction specific access to a secured resource having a secured resource identity (the “Accused Instrumentality”). The Vantage transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The

requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



Detailed Features

1 DIGITAL WALLET

Your new card can make life a little easier, and help keep your financial information more secure.

[VIEW DEMO](#)

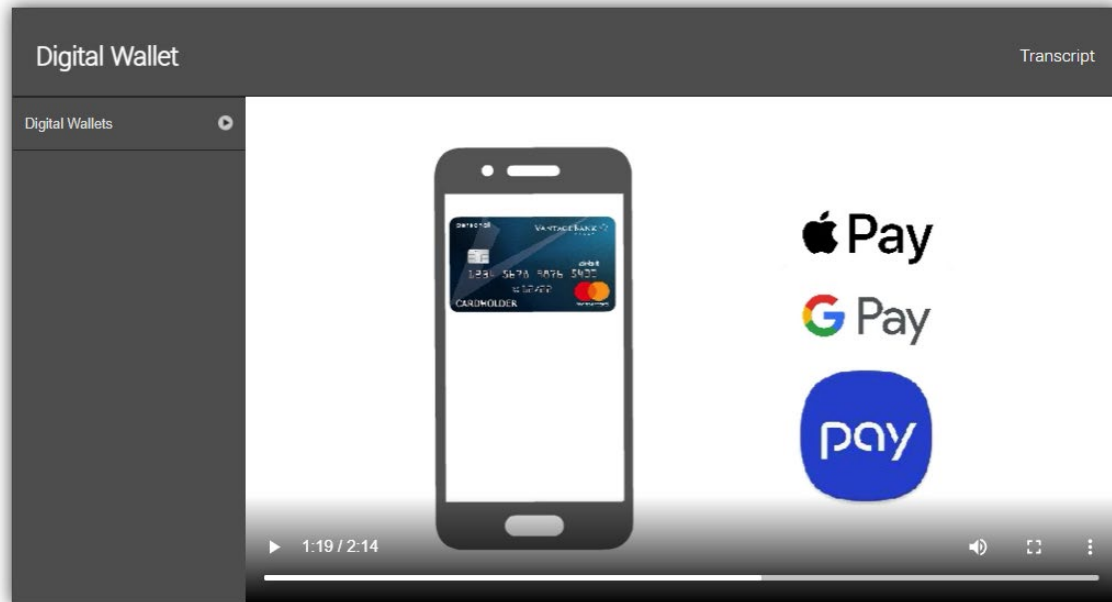
2 POPMONEY®

3 MOBILE CHECK DEPOSIT

4 CARD VALET

5 NOTIFI FOR MOBILE

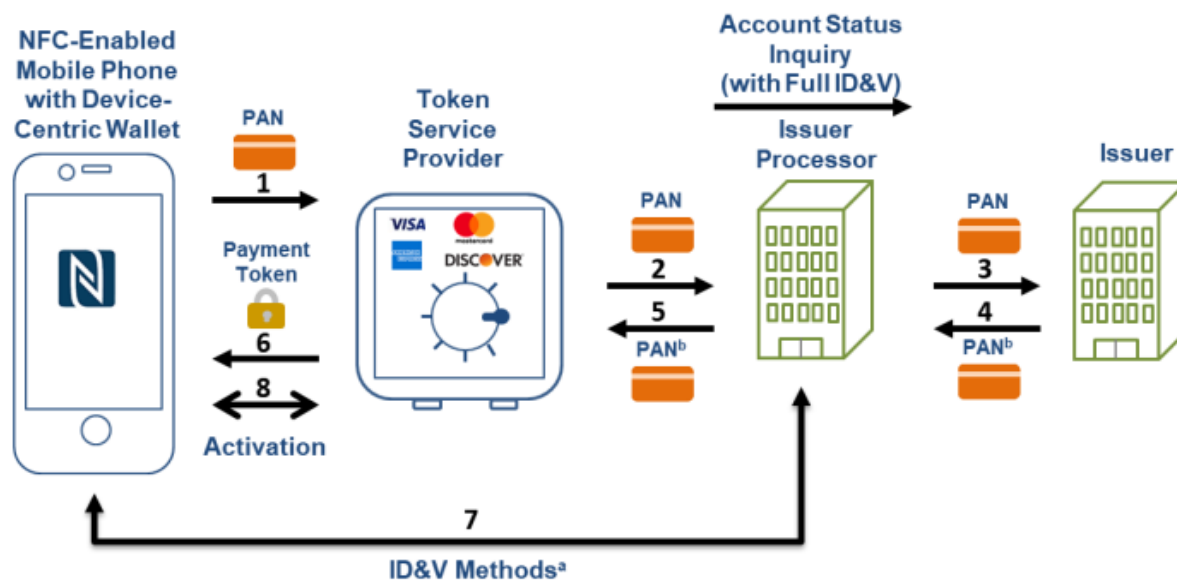
(Source: <https://www.vantage.bank/en/digital/vantage-personal-mobile/>)



(Source: <https://www.onlinebanktours.com/mobile/?b=6591&c=80164>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

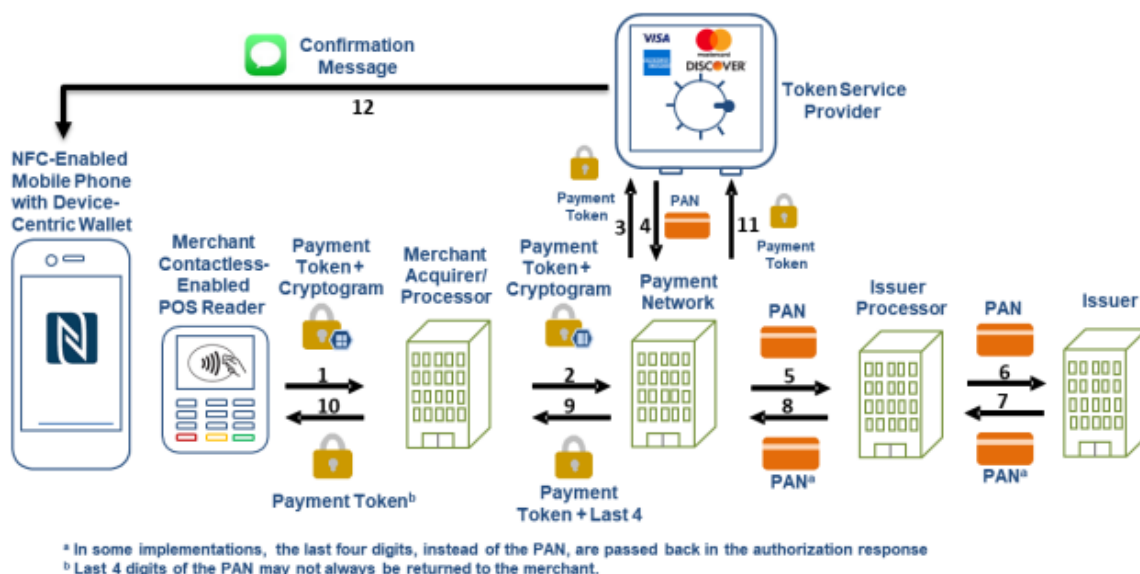


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

71. Vantage's use of the Accused Instrumentality includes a method for authorizing transaction specific access to a secured resource having a secured resource identity. For example, a Vantage account holder requests Vantage to provision a specific Vantage debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Vantage card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's

smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram.

72. The Accused Instrumentality includes receiving at a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive a request for transaction specific access to a secured resource by a service client. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by Vantage card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Vantage card account of the account holder. This messaging gateway is either hosted directly by Vantage or through an agent with whom Vantage has contracted to receive the messages.

73. The Accused Instrumentality includes generating a key string with a server in communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate the key string known to both said server and an authorized user of the secured resource, said key string being associated with the secured resource within a key string table accessible by the server and providing a basis for authenticating the secured resource identity by searching the key string table for the key string. For example, behind the firewall of the messaging gateway and in communication therewith is an authorization server that generates a token corresponding to a secured resource during the

provisioning process. After this, the authorization server updates a table that maps token numbers to secured resource identities. The authorization server is then able to search the table to authenticate a secured resource identity by searching the table for the token. If the token has a corresponding secured resource identity, that identity is authenticated. The authorization server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to provide the authentication services.

74. The Accused Instrumentality includes determining transaction specific information with the server in communication with the messaging gateway, the server having a third set of instructions embodied in a computer readable medium operable to identify transaction specific information within the request. For example, the authorization server is also programmed to identify within the payment authorization request transaction specific information that was passed by the merchant. The authorization server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to provide the authentication services.

75. The Accused Instrumentality includes communicating said key string to said authorized user. For example, once the provisioning process is complete, the messaging gateway and/or the server send the token to the authorized user's mobile device. The messaging gateway is either hosted directly by Vantage or through an agent with whom Vantage has contracted to provide the authentication services. The authorization server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to provide the authentication services.

76. The Accused Instrumentality includes receiving an authentication credential from said service client, said authentication credential having been provided to said service client by said authorized user. For example, the authorization server is also programmed to identify within

the payment authorization request the cryptogram that was passed by the user to the merchant. The authorization server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to provide the authentication services.

77. The Accused Instrumentality includes evaluating said authentication credential. For example, the authorization server uses the token value and other transaction information received to evaluate the cryptogram. If the cryptogram is valid, the authorization server authorizes the transaction specific access. The authorization server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to provide the authentication services.

78. The Accused Instrumentality includes wherein the key string and authentication credential do not reveal any primary identifier associated with said secured resource. For example, neither the token nor the cryptogram reveals the debit and/or credit card number associated with the secured resource.

79. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

80. Defendants thus infringe one or more claims of the 499 Patent. The elements and conduct described herein are covered by and infringe upon at least Claim 3 of the 499 Patent.

Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 499 Patent.

81. Vantage has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

82. Vantage has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 499 Patent by others and Vantage will continue to do so unless enjoined by this Court. Vantage's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 499 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Vantage knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 499 Patent.

83. Vantage continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers,

businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 499 Patent.

84. Vantage has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 3 of the 499 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 499 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

85. Vantage has committed these acts of infringement without license or authorization.

86. By engaging in the conduct described herein, Vantage has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Vantage is thus liable to Textile for infringement of the 499 Patent, pursuant to 35 U.S.C. § 271.

87. As a direct and proximate result of Vantage's infringement of the 499 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Vantage's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

88. In addition, the infringing acts and practices of Vantage have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate

and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Vantage is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Vantage is finally and permanently enjoined from further infringement.

89. Vantage has had actual knowledge of the 499 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Vantage will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 499 Patent.

90. Vantage has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 499 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

91. Textile has been damaged as a result of the infringing conduct by Vantage alleged above. Thus, Vantage is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

92. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 499 Patent.

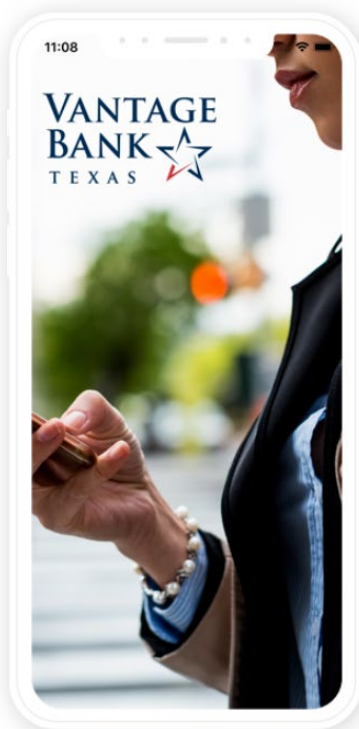
COUNT IV

INFRINGEMENT OF U.S. PATENT NO. 10,148,659

93. On December 4, 2018, United States Patent No. 10,148,659 (“the 659 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

94. Textile is the owner of the 659 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 659 Patent against infringers, and to collect damages for all relevant times.

95. Vantage offers debit and/or credit cards, such as the Vantage Bank Texas Visa and Mastercard Credit Cards, that are used with a computer-implemented system for a credit or debit and/or credit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit and/or credit card account number to the merchant (the “Accused Instrumentality”). The Vantage transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user’s debit and/or credit card number so that the user’s debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user’s debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user’s smartphone by the system, and wherein each account held by the user has its own token.



Detailed Features

1 DIGITAL WALLET

Your new card can make life a little easier, and help keep your financial information more secure.

[VIEW DEMO](#)

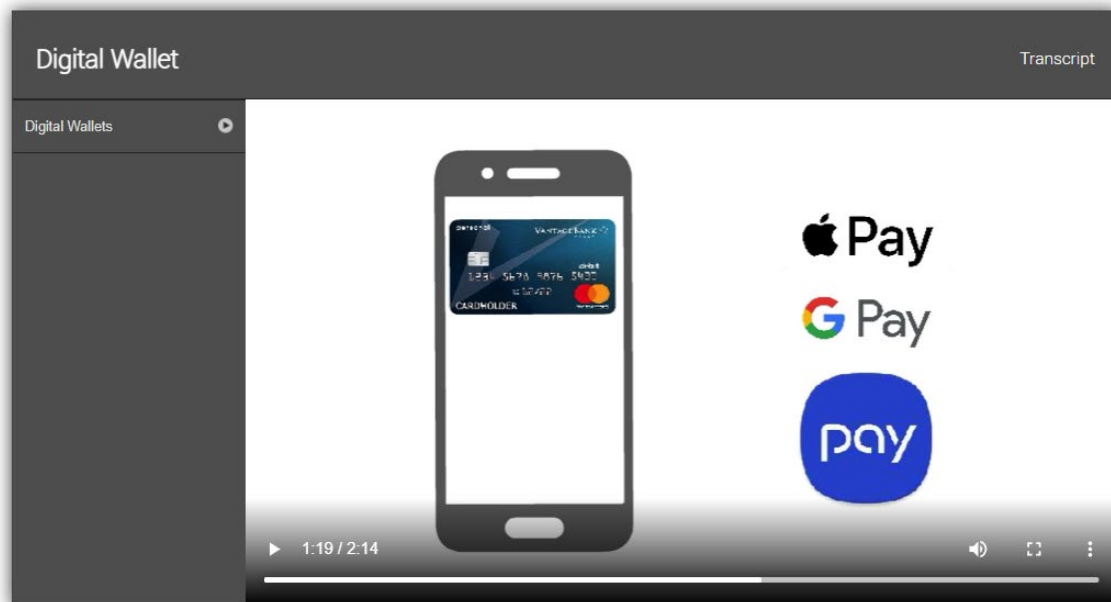
2 POPMONEY®

3 MOBILE CHECK DEPOSIT

4 CARD VALET

5 NOTIFI FOR MOBILE

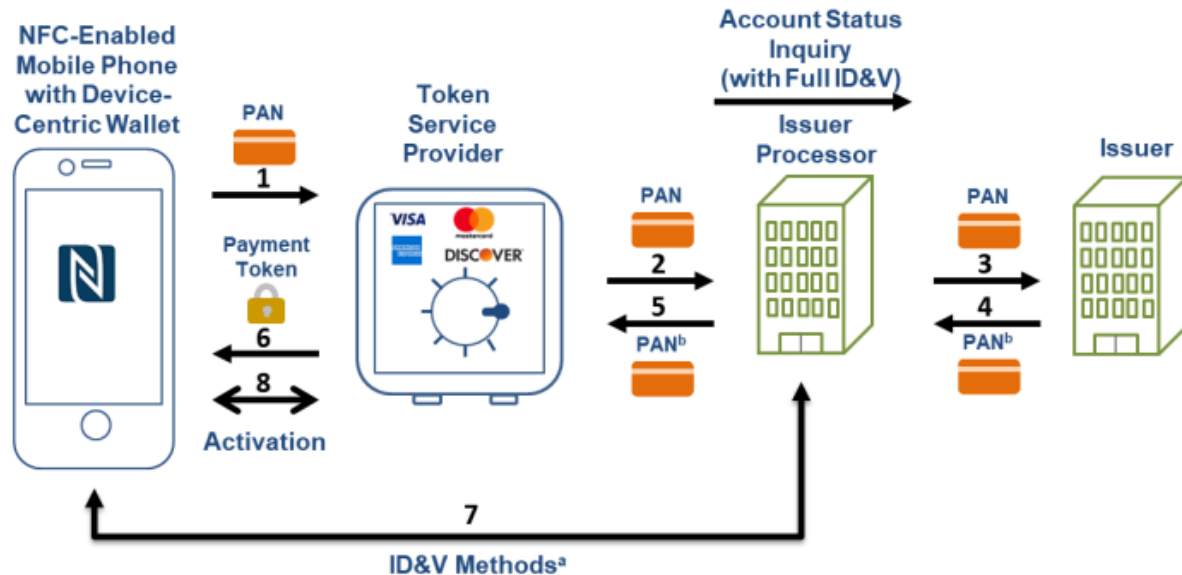
(Source: <https://www.vantage.bank/en/digital/vantage-personal-mobile/>)



(Source: <https://www.onlinebanktours.com/mobile/?b=6591&c=80164>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^a ID&V methods includes text or email or call. OTP is an example.

^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

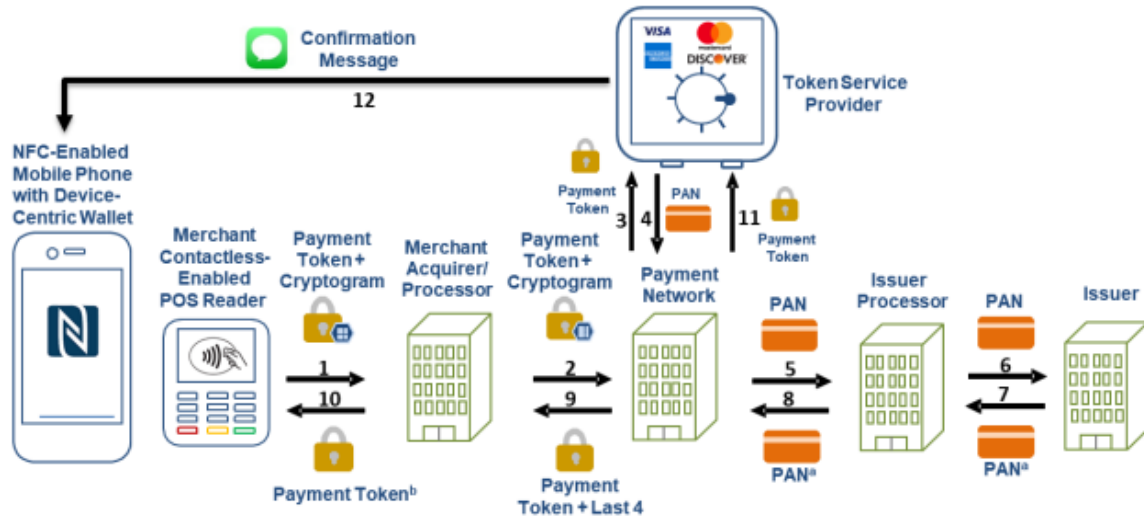
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

96. The Accused Instrumentality includes a computer-implemented system for a credit or debit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit card account number to the merchant. For example, a Vantage account holder requests Vantage to provision a specific Vantage debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Vantage to a specific merchant in a specific amount for a specific transaction from a specific

Vantage card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

97. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a credit or debit card account holder's mobile device, a merchant's payment application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a Vantage card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Vantage card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Vantage card account of the account holder. This interface is either hosted directly by Vantage or through an agent with whom Vantage has contracted to receive the messages.

98. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration

information received from the credit or debit card account holder through the at least one interface, the registration information comprising a credit or debit card account holder identifier and at least one credit or debit card account number having an associated unique account identifier wherein the credit or debit card account number and unique account identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card and the debit and/or credit card account number (which has a corresponding token), received from Vantage card account holders through the interface for provisioning a specific Vantage debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Vantage card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Vantage card account of the account holder. The server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to receive the messages.

99. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to pay the specific merchant for the specific transaction from a given debit or credit card account, the authorization request message having been received through the at least one interface and originating from the credit or debit card account holder's mobile device and comprising: a first merchant identifier; a first transaction specific information selected from the group consisting of a first transaction amount and first client reference identifier; the credit or debit card account holder identifier; and a designated unique account identifier selected from the at least one unique account identifiers. For example, the Accused

Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Vantage card account holder's mobile device. The server is programmed to receive authorization requests initiated by Vantage card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a merchant identifier, and the Vantage card account holder identifier. The server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to receive the messages.

100. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string wherein the key string is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the designated unique account identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to receive the messages.

101. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive a payment request message from the merchant's payment application through the at least one interface, the payment request message comprising: a second merchant identifier; a second transaction specific information selected from the group consisting of a second transaction amount and second client reference identifier; and a second transaction specific authentication credential whereby the second authentication credential was received by the merchant application from the credit or debit card account holder's mobile device. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Vantage card account holder's mobile device. The server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to receive the messages.

102. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the credit or debit card account holder's request to use the credit or debit card account number associated with the designated unique account identifier for payment to the specific merchant for the specific transaction and authorizing the resource provider to use the credit or debit card account number associated with the designated unique account identifier to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or bank account number to the

specific merchant by determining if: the first merchant identifier matches the second merchant identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to provide the authentication services.

103. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

104. Defendants thus infringe one or more claims of the 659 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 9 of the 659 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 659 Patent.

105. Vantage has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. §

271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

106. Vantage has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 659 Patent by others and Vantage will continue to do so unless enjoined by this Court. Vantage's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 659 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Vantage knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 659 Patent.

107. Vantage continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 659 Patent.

108. Vantage has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 659 Patent by others, such as

consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

109. Vantage has committed these acts of infringement without license or authorization.

110. By engaging in the conduct described herein, Vantage has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Vantage is thus liable to Textile for infringement of the 659 Patent, pursuant to 35 U.S.C. § 271.

111. As a direct and proximate result of Vantage's infringement of the 659 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Vantage's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

112. In addition, the infringing acts and practices of Vantage have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Vantage is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Vantage is finally and permanently enjoined from further infringement.

113. Vantage has had actual knowledge of the 659 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Vantage will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 659 Patent.

114. Vantage has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 659 Patent, as explained further below in the “Additional Allegations Regarding Infringement” section.

115. Textile has been damaged as a result of the infringing conduct by Vantage alleged above. Thus, Vantage is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

116. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 659 Patent.

COUNT V

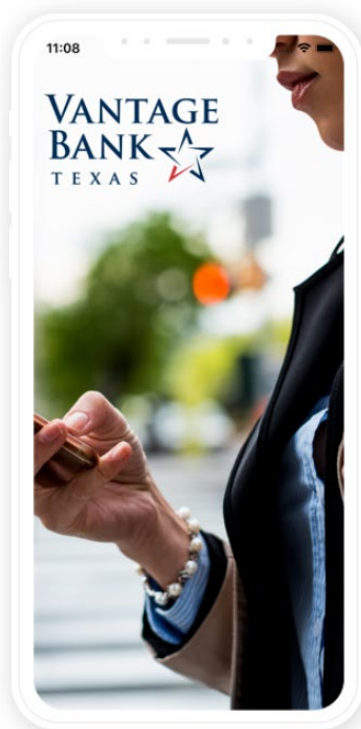
INFRINGEMENT OF U.S. PATENT NO. 10,560,454

117. On February 11, 2020, United States Patent No. 10,560,454 (“the 454 Patent”) was duly and legally issued by the United States Patent and Trademark Office for an invention entitled “Authentication System and Method.”

118. Textile is the owner of the 454 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 454 Patent against infringers, and to collect damages for all relevant times.

119. Vantage offers debit and/or credit cards, such as the Vantage Bank Texas Visa and Mastercard Credit Cards, that are used with a computer-implemented system for a user to

authorize a resource authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client (the "Accused Instrumentality"). The Vantage transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



Detailed Features

1 DIGITAL WALLET

Your new card can make life a little easier, and help keep your financial information more secure.

[VIEW DEMO](#)

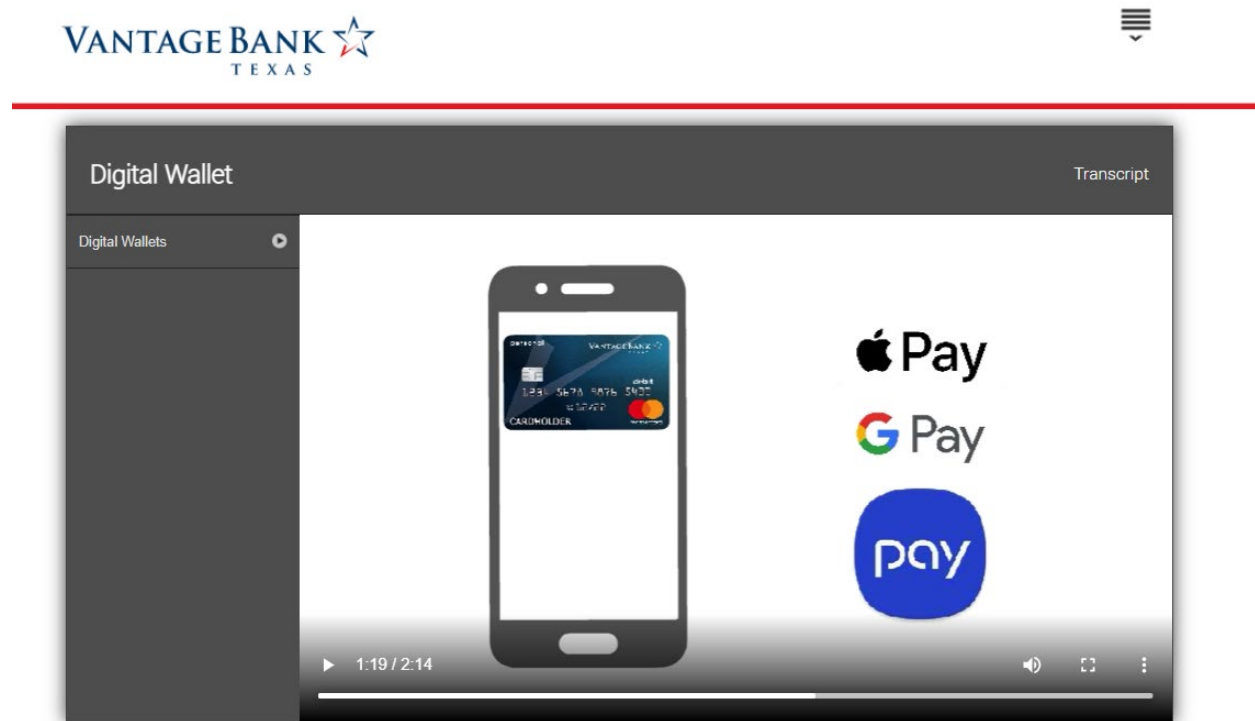
2 POPMONEY®

3 MOBILE CHECK DEPOSIT

4 CARD VALET

5 NOTIFI FOR MOBILE

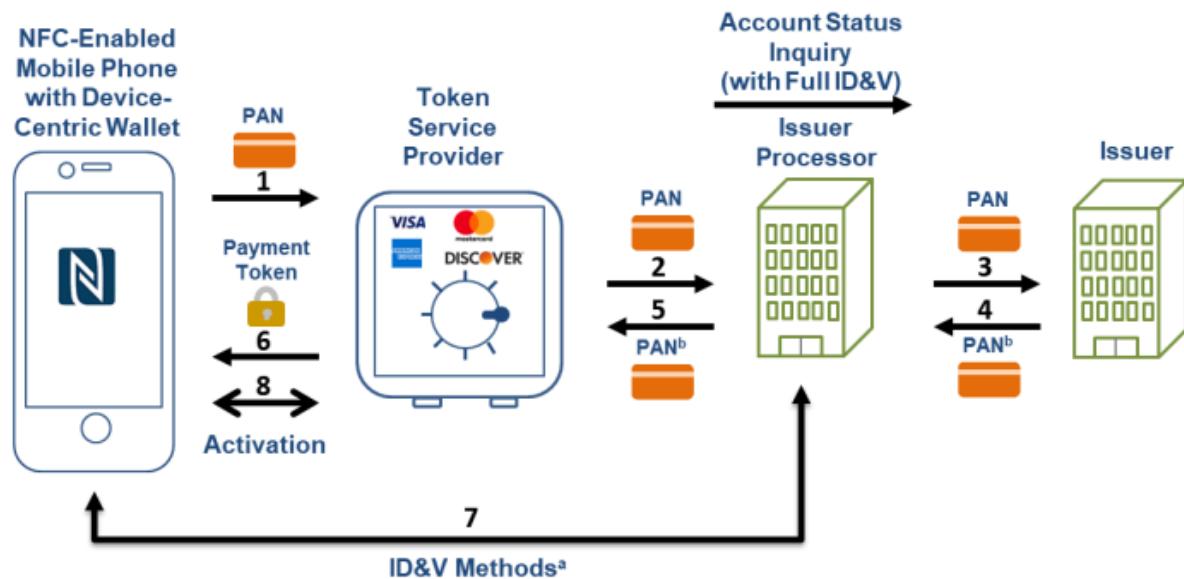
(Source: <https://www.vantage.bank/en/digital/vantage-personal-mobile/>)



(Source: <https://www.onlinebanktours.com/mobile/?b=6591&c=80164>)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



^aID&V methods includes text or email or call. OTP is an example.

^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

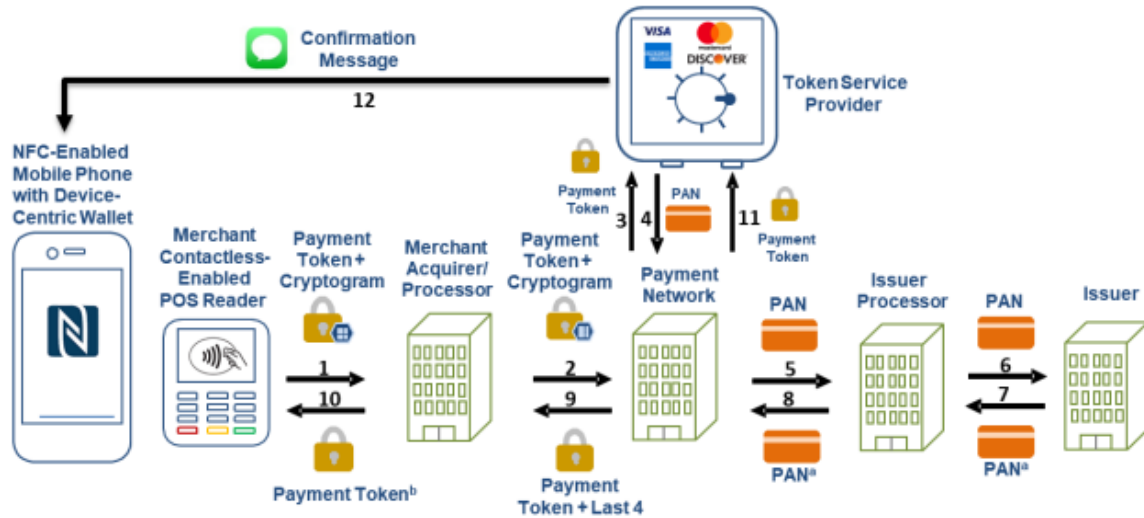
ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response

^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN⁶ to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: <https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf>)

120. The Accused Instrumentality includes a computer-implemented system for a user to authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client. For example, a Vantage account holder requests Vantage to provision a specific Vantage debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by Vantage to a specific merchant in a specific amount for a specific transaction from a specific Vantage card account of the account holder using his or her

smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

121. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a user's application, a service client's application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a Vantage card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by Vantage card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Vantage card account of the account holder. This interface is either hosted directly by Vantage or through an agent with whom Vantage has contracted to receive the messages.

122. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration information received from the user through the at least one interface, the registration information comprising a user identifier and at least one secured resource identifier associated with the

common identifier of the secured resource, wherein the common identifier and secured resource identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card, the debit and/or credit card account number (which has a corresponding token), and the CVV number received from Vantage card account holders through the interface for provisioning a specific Vantage debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by Vantage card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific Vantage card account of the account holder. The server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to receive the messages.

123. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to authorize access to the secured resource by the service client, the authorization request message having been received through the at least one interface from the user's application and comprising: a first service client identifier; a first transaction specific information; the user identifier; and a designated secured resource identifier selected from one of the at least one secured resource identifiers. For example, the Accused Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the Vantage card account holder's mobile device. The server is programmed to receive authorization requests initiated by Vantage card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction,

a token, a CVV number, a merchant identifier, other token information, and the Vantage card account holder identifier. The server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to receive the messages.

124. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string and does not include or reveal the common identifier associated with the designated secured resource identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to receive the messages.

125. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive an access request message from the service client's application through the at least one interface, the payment request message comprising: a second service client identifier; a second transaction specific information; and a second transaction specific authentication credential whereby the second transaction specific authentication credential was received by the service client's

application from the user's application. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the Vantage card account holder's mobile device. The server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to receive the messages.

126. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the user's request to access the secured resource associated with the designated secured resource identifier without transmitting or otherwise providing the common identifier of the secured resource to the service client by determining if: the first service client identifier matches the second service client identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by Vantage or through an agent with whom Vantage has contracted to provide the authentication services.

127. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

128. Defendants thus infringe one or more claims of the 454 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 8 of the 454 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 454 Patent.

129. Vantage has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

130. Vantage has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 454 Patent by others and Vantage will continue to do so unless enjoined by this Court. Vantage's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused

Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 454 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. Vantage knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 454 Patent.

131. Vantage continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 454 Patent.

132. Vantage has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 454 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

133. Vantage has committed these acts of infringement without license or authorization.

134. By engaging in the conduct described herein, Vantage has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and Vantage is thus liable to Textile for infringement of the 454 Patent, pursuant to 35 U.S.C. § 271.

135. As a direct and proximate result of Vantage's infringement of the 454 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for Vantage's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

136. In addition, the infringing acts and practices of Vantage have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which Vantage is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that Vantage is finally and permanently enjoined from further infringement.

137. Vantage has had actual knowledge of the 454 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, Vantage will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 454 Patent.

138. Vantage has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 454 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

139. Textile has been damaged as a result of the infringing conduct by Vantage alleged above. Thus, Vantage is liable to Textile in an amount that adequately compensates it for such

infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

140. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 454 Patent.

ADDITIONAL ALLEGATIONS REGARDING INFRINGEMENT

141. Vantage has also indirectly infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by inducing others to directly infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Vantage has induced the end-users, Vantage's customers, to directly infringe (literally and/or under the doctrine of equivalents) the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by using the Accused Instrumentality.

142. Vantage took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

143. Such steps by Vantage included, among other things, advising or directing customers and end-users to use the Accused Instrumentality in an infringing manner; advertising and promoting the use of the Accused Instrumentality in an infringing manner; and/or distributing instructions that guide users to use the Accused Instrumentality in an infringing manner.

144. Vantage has performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454

Patent and with the knowledge that the induced acts constitute infringement, at least since the filing of the Complaint.

145. Vantage was and is aware that the normal and customary use of the Accused Instrumentality by Vantage's customers would infringe the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Vantage's inducement is ongoing.

146. Vantage directs or controls the use of the Accused Instrumentality nationwide through its own websites and in its own branches, including in Texas and elsewhere in the United States, and expects and intends that the Accused Instrumentality will be so used.

147. Vantage took active steps, directly and/or through contractual relationships with others, with the specific intent to cause such persons to make or use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

148. Vantage performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts would constitute infringement.

149. Vantage's inducement is ongoing.

150. Vantage has also indirectly infringed by contributing to the infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent. Vantage has contributed to the direct infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by the end-user of the Accused Instrumentality.

151. The Accused Instrumentality has special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the 079

Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 3 of the 499 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

152. As described above, the special features include securely authorizing specific transactions without providing a credit or debit card number to the merchant used in a manner that infringes the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

153. The special features constitute a material part of the invention of one or more of the claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent and are not staple articles of commerce suitable for substantial non-infringing use.

154. Vantage's contributory infringement is ongoing.

155. Vantage's actions are at least objectively reckless as to the risk of infringing valid patents and this objective risk was either known or should have been known by Vantage, at least since the filing of the Complaint.

156. Vantage has had knowledge of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent at least since the filing of the Complaint.

157. Vantage's customers have infringed the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent.

158. Vantage encouraged its customers' infringement.

159. Vantage's direct and indirect infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent is, has been, and/or continues to be willful, intentional, deliberate, and/or in conscious disregard of Textile's rights under the patents.

160. Textile has been damaged as a result of the infringing conduct by Vantage alleged above. Thus, Vantage is liable to Textile in an amount that adequately compensates it for such

infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Textile hereby requests a trial by jury on all issues so triable by right.

PRAYER FOR RELIEF

Textile requests that the Court find in its favor and against Vantage, and that the Court grant Textile the following relief:

- a. Judgment that one or more claims of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent have been infringed, either literally and/or under the doctrine of equivalents, by Vantage and/or all others acting in concert therewith;
- b. A permanent injunction enjoining Vantage and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert therewith from infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent; or, in the alternative, an award of a reasonable ongoing royalty for future infringement of the 079 Patent, the 802 Patent, the 499 Patent, the 659 Patent, and the 454 Patent by such entities;
- c. Judgment that Vantage account for and pay to Textile all damages to and costs incurred by Textile because of Vantage's infringing activities and other conduct complained of herein, including an award of all increased damages to which Textile is entitled under 35 U.S.C. § 284;
- d. That Textile be granted pre-judgment and post-judgment interest on the damages caused by Vantage's infringing activities and other conduct complained of herein;
- e. That this Court declare this an exceptional case and award Textile its reasonable

attorney's fees and costs in accordance with 35 U.S.C. § 285; and

f. That Textile be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: October 12, 2021

Respectfully submitted,

/s/ Matthew J. Antonelli

Matthew J. Antonelli

Texas Bar No. 24068432

matt@ahtlawfirm.com

Zachariah S. Harrington

Texas Bar No. 24057886

zac@ahtlawfirm.com

Larry D. Thompson, Jr.

Texas Bar No. 24051428

larry@ahtlawfirm.com

Christopher Ryan Pinckney

Texas Bar No. 24067819

ryan@ahtlawfirm.com

ANTONELLI, HARRINGTON

& THOMPSON LLP

4306 Yoakum Blvd., Ste. 450

Houston, TX 77006

(713) 581-3000

Stafford Davis

State Bar No. 24054605

sdavis@stafforddavisfirm.com

Catherine Bartles

Texas Bar No. 24104849

cbartles@stafforddavisfirm.com

THE STAFFORD DAVIS FIRM

815 South Broadway Avenue

Tyler, Texas 75701

(903) 593-7000

(903) 705-7369 fax

Of Counsel:

Sandeep Seth

Texas State Bar No. 18043000

SETHLAW

Pennzoil Place

700 Milam Street, Suite 1300

Houston, Texas 77002
Telephone: (713) 244-5017
ss@sethlaw.com

Attorneys for Textile Computer Systems, Inc.